

# **A Computerized Operator Support System Prototype**

Ken Thomas  
Ronald Boring  
Roger Lew  
Tom Ulrich  
Richard Vilim

November 2013



The INL is a U.S. Department of Energy National Laboratory  
operated by Battelle Energy Alliance

#### **DISCLAIMER**

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

# **A Computerized Operator Support System Prototype**

**Ken Thomas, Ronald Boring, Roger Lew, Tom Ulrich, Idaho National Laboratory**

**Richard Vilim, Argonne National Laboratory**

**Idaho National Laboratory  
Idaho Falls, Idaho 83415**

**<http://www.inl.gov>**

**Prepared for the  
U.S. Department of Energy  
Office of Nuclear Energy  
Under DOE Idaho Operations Office  
Contract DE-AC07-05ID14517**



## Executive Summary

A report was published by the Idaho National Laboratory in September of 2012, entitled *Design to Achieve Fault Tolerance and Resilience*, which described the benefits of automating operator actions for transients. The report identified situations in which providing additional automation in lieu of operator actions would be advantageous. It recognized that managing certain plant upsets is sometimes limited by the operator's ability to quickly diagnose the fault and to take the needed actions in the time available.

Undoubtedly, technology is underutilized in the nuclear power industry for operator assistance during plant faults and operating transients. In contrast, other industry sectors have amply demonstrated that various forms of operator advisory systems can enhance operator performance while maintaining the role and responsibility of the operator as the independent and ultimate decision-maker.

A computerized operator support system (COSS) is proposed for use in nuclear power plants to assist control room operators in addressing time-critical plant upsets. A COSS is a collection of technologies to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. The COSS does not supplant the role of the operator, but rather provides rapid assessments, computations, and recommendations to reduce workload and augment operator judgment and decision-making during fast-moving, complex events.

This project proposes a general model for a control room COSS that addresses a sequence of general tasks required to manage any plant upset: detection, validation, diagnosis, recommendation, monitoring, and recovery. The model serves as a framework for assembling a set of technologies that can be interrelated to assist with each of these tasks.

A prototype COSS has been developed in order to demonstrate the concept and provide a test bed for further research. The prototype is based on four underlying elements consisting of a digital alarm system, computer-based procedures, PI&D system representations, and a recommender module for mitigation actions. At this point, the prototype simulates an interface to a sensor validation module and a fault diagnosis module. These two modules will be fully integrated in the next version of the prototype.

The initial version of the prototype is now operational at the Idaho National Laboratory using the U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) Human Systems Simulation Laboratory (HSSL). The HSSL is a full-scope, full-scale glass top simulator capable of simulating existing and future nuclear power plant main control rooms. The COSS is interfaced to the Generic Pressurized Water Reactor (gPWR) simulator with industry-typical control board layouts. The glass top panels display realistic images of the control boards that can be operated by touch gestures. A section of the simulated control board was dedicated to the COSS human-system interface (HSI), which resulted in a seamless integration of the COSS into the normal control room environment.

Two COSS demonstration scenarios have been developed for the prototype involving the Chemical & Volume Control System (CVCS) of the PWR simulator. The first involves a primary coolant leak outside of containment which would require tripping the reactor if not mitigated in a very short timeframe. The COSS prototype presents a series of operator screens that provide the needed information and soft controls to successfully mitigate the event.

The second involves the trip of a Charging and Safety Injection Pump (CSIP), which results in a decreasing pressurizer level and would ultimately lead to a reactor trip. The COSS prototype presents a series of options to start an alternate CSIP and thereby mitigate the event.

The prototype is intended to be further developed in future years based on additional research in the areas of enhanced plant instrumentation, real-time sensor validation and fault diagnosis, and COSS human factors evaluations.

# Table of Contents

Executive Summary .....	ii
Table of Contents .....	iv
LIST OF FIGURES .....	viii
LIST OF TABLES .....	ix
ACRONYMS .....	x
1. Introduction .....	1
2. Computerized Operator Support Systems .....	3
2.1 Concept .....	3
2.2 Relevant COSS Examples .....	3
2.2.1 Early German Nuclear Plant COSS .....	4
2.2.2 Halden Reactor Project's Operator Assistant .....	4
2.2.3 Eascon Operator Advisory System .....	5
2.2.4 Traffic Collision Avoidance System (TCAS) .....	5
2.2.5 Terrain Avoidance and Warning System (TAWS) .....	6
2.3 Relevance to NPP Control Room Operator Performance .....	7
3. CVCS COSS Conceptual Model for Fault Management .....	10
3.1 General Concept .....	10
3.1.1 Overview of COSS Features .....	11
3.1.2 Observance of Licensed Operator Duties and Responsibilities .....	12
3.2 Sensor Validation .....	13
3.3 Fault Detection and Diagnosis .....	15
3.4 Fault Mitigation .....	17
3.5 Monitoring .....	18
3.6 Recovery .....	19
4. Computerized Operator Support System Prototype Development .....	20
4.1 COSS Design .....	20
4.1.1 Design Elements .....	20
4.1.2 Design Philosophy .....	21
4.1.3 Design Process .....	22
4.2 Technical Considerations .....	22
4.2.1 Full Scope Simulation Environment .....	22
4.2.2 Software Development Environment .....	23
4.3 COSS Prototype .....	24
4.3.1 Display Overview .....	24
4.3.2 Status Indicator and Menu .....	27
4.3.3 COSS Recommender System .....	28

4.3.4	Computer-Based Procedures.....	29
4.3.5	Piping and Instrumentation Diagrams.....	30
4.3.6	Trend Alarm Panel.....	31
4.3.7	Navigation.....	34
4.4	Leaking Demineralizer Scenario Walkthrough.....	34
4.4.1	Fault Detection.....	34
4.4.2	Fault Validation and Diagnosis.....	36
4.4.3	Fault Mitigation.....	36
4.4.4	Fault Monitoring and Validation.....	42
4.4.5	Resume Normal Operations Suggestions.....	42
4.5	CSIP Trip Scenario Walkthrough.....	42
4.5.1	Fault Detection.....	42
4.5.2	Fault Validation and Diagnosis.....	43
4.5.3	Fault Mitigation.....	44
4.5.4	Fault Monitoring and Validation.....	46
4.5.5	Resume Normal Operations Suggestions.....	46
5.	Future Research.....	48
5.1	Real-Time Interface with Sensor Validation and Fault Diagnosis.....	48
5.2	Enhanced Plant Instrumentation.....	48
5.3	Real-time Sensor Validation and Fault Diagnosis.....	48
5.4	COSS Human Factors Evaluation.....	50
6.	References.....	54
	Appendix A: Computerized Operator Support System Specifications.....	55
A.1	General COSS Interface Specifications.....	55
	Purpose.....	55
	Design Assumptions.....	55
	Design Requirements.....	55
A.2	Computer-based Procedures Specifications.....	55
	Purpose.....	55
	Design Assumptions.....	56
	Design Requirements.....	56
A.3	P&ID Display Specifications.....	57
	Purpose.....	57
	Design Assumptions.....	57
	Design Requirements.....	58
A.4	Recommender System Specifications.....	58
	Purpose.....	58
	Design Assumptions.....	58
	Design Requirements.....	58
A.5	Trend Alarms Specifications.....	59
	Purpose.....	59
	Design Assumptions.....	59
	Design Requirements.....	60
A.6	Navigation Specifications.....	60
	Purpose.....	60
	Design Assumptions.....	60



	Design Requirements .....	60
A.7	COSS Status Display Specifications .....	61
	Purpose61	
	Design Assumptions .....	61
	Design Requirements .....	61



## LIST OF FIGURES

Figure 1 COSS Interface with operators and plant systems.....	12
Figure 2 Regenerative heat exchanger.....	14
Figure 3 Screenshot from the AFTR-MSET test stand.....	15
Figure 4 Screenshot of a simplified PRODIAG representation of a CVCS.....	17
Figure 5 Current DCS for CVCS from a modernized control room at a nuclear power plant.....	21
Figure 6 A development team member at the helm of the early CVCS COSS prototype embedded in the HSSL. ....	23
Figure 7 Early prototype of a CVCS COSS display of the P&ID mode during a normal operating state.....	25
Figure 8 Annotated more advanced COSS DVCS display prototype. During normal operating states the warning and message areas of the recommender system are blank. ....	26
Figure 9 COSS P&ID main window depicting the CVCS and interconnected systems during a normal operating state. ....	27
Figure 10 COSS status indicator and navigation buttons.....	28
Figure 11 Recommender system presenting a warning with the shot clock and diagnosing the fault.....	28
Figure 12 Shot clock tooltip.....	29
Figure 13 Recommender message section containing "Show Me" buttons that link to the P&ID and procedure and the disregard button. Also present is the "Enable Reset" and "Reset COSS" buttons.....	29
Figure 14 Computer-based procedure depicting the active step with a light grey background, a step status message, and a "Go to step" button in the active state.....	30
Figure 15 COSS display featuring suggested mitigation actions and components related to the fault and the mitigation of the fault. ....	31
Figure 16 COSS display featuring trend alarms that have reached warning, alarm, and sensor drift and failure states. ....	33
Figure 17 Expanded trend view from one of the trend alarms.....	33
Figure 18 COSS display depicting multiple selectable tabs for different computer-based procedures.....	34
Figure 19 COSS display featuring the recommender during the initial detection of a fault.....	35
Figure 20 COSS display featuring the recommender identifying the leak and suggesting mitigation actions. ....	36
Figure 21 CBP displaying the purpose and entry conditions for AOP-016.....	37
Figure 22 Computer-based procedure displaying the first step of AOP-016.....	37
Figure 23 Computer-based procedure depicting a step that requires the operator to enter another operating procedure before continuing the current procedure.....	38

Figure 24 Computer-based procedure depicting procedure tabs and an exit procedure button. ....	39
Figure 25 Computer-based procedures depicting a manually selected valve diverting and the associated in progress indicator. ....	40
Figure 26 Computer-based procedure depicting the selection of the "Resume AE to step 4b." button and the feedback indicating automatic execution is enacted. ....	41
Figure 27 Computer-based procedures depicting the "Automatic execution of steps 4a through 4b." initiated by selecting the run button located along the bottom of the display.....	41
Figure 28 COSS display featuring the validated resolution of the coolant leak and the option to navigate to suggested recovery actions.....	42
Figure 29 COSS warning area stating the CSIP A Trip, recommender diagnosing status, and CSIP A highlight on the P&ID. ....	43
Figure 30 COSS recommender displaying the option to enter the APP-ALB-06 CBP because the cause of the pump trip could not be identified.....	44
Figure 31 COSS depicting the validation of the mitigation actions taken to start CSIP B and restore charging flow. ....	45
Figure 32 CBP view depicting the CSIP A failure to restart message in the information box and the automatic activation of the buttons in the response not obtained column. ....	45
Figure 33 A lock out tag out symbol is overlaid on the breaker for CSIP A after the operator selects the “Disregard” button next to the recommender message “Disregard the warning for 5 minutes”. ....	46
Figure 34 Lock out tag out dialog contained detailed information about CSIP A.....	47

## LIST OF TABLES

Table 1. COSS Functions. ....	11
-------------------------------	----

## **ACRONYMS**

AE	Automatic Execution
AFTR-MSET	Algorithm for Transient Multivariable Sensor Estimation
AOPs	Abnormal Operating Procedures
CBP	Computer-based Procedure
COPS	Computerized Operating Procedure Systems
COSS	Computerized Operator Support System
CSIP	Charging and Safety Injection Pump
CVCS	Chemical and Volume Control Systems
DCS	Digital Control System
EOP	Emergency Operations Procedures
FAA	Federal Aviation Administration
GPS	Global Positioning System
gPWR	Generic Pressurized Water Reactor
HRP	Halden Reactor Project
HSIs	Human System Interfaces
HSSL	Human Systems Simulation Laboratory
IAEA	International Atomic Energy Agency
IGCC	Integrated Gasification Combined Cycle
INPO	Institute for Nuclear Power Operations
LWRS	Light Water Reactor Sustainability
MEM	Mass, Energy, and Momentum
NPP	Nuclear Power Plants
NRC	Nuclear Regulatory Commission
OECD	Organization for Economic Co-Operation and Development
OPC	Object Linking and Embedding for Process Control
P&ID	Piping and Instrumentation Diagram
PSA	Probabilistic Safety Analysis
PRODIAG	Process Diagnostics
RAs	Resolution Advisories
RCS	Reactor Coolant System
RHR	Residual Heat Removal
SOER	Significant Operating Experience Report
SOP	Standard Operation Procedures

TAs	Traffic Advisories
TAWS	Terrain Avoidance and Warning System
TCAS	Traffic Collision Avoidance Systems
TH	Thermal-Hydraulic
VCT	Volume Control Tank
WPF	Windows Presentation Foundation

# 1. Introduction

For nuclear power plants, there is a trade-off in control philosophy between automatic system control and operator control, reflecting a complex set of factors. Some automatic systems are used when there is insufficient time for operators to diagnose and respond to fast-moving events. The plant operates in an envelope of conditions that are supervised by the plant protection system, in the form of setpoints for protective actions that will be automatically invoked if the thresholds are exceeded. These automatic actions generally have to be conservative to stay ahead of plant events, and are designed to put the plant in a safe and known condition, such as a reactor trip. Other automatic actions are part of the plant control system, and maintain important plant parameters at the desired operating points by making some adjustments to plant components such as valve positions and pump speeds. These control actions relieve the plant operators from the burden of continuous, tedious manual control of these components.

In less time-critical and more nuanced situations operator actions are preferred because it is especially important to keeping the plant on-line if possible. These situations occur with higher frequency and are less severe than those dealt with by the current plant protection system. In these situations human operators are superior at diagnosing the causes of the situation and performing mitigations that preserve the margin of safety without being overly conservative. Rather than trying to enhance operator response to these situations through automation, the industry has rather focused on making these events less frequent by investing in equipment reliability and redundancy. However, these types of events continue to happen in spite of the focus on equipment reliability.

A report was published by the INL in September of 2012, entitled *Design to Achieve Fault Tolerance and Resilience*, which described the benefits of automating operator actions for transients. The report identified situations where there are alternate configurations and actions that can mitigate the need for a safety actuation if there is time to do so [1]. These situations are sometimes limited by the ability of the operator to accurately diagnose the cause of the upset and to take the needed actions in the available time. The ability to accurately diagnose the situation is, in turn, often limited by the available instrumentation to characterize the fault and the ability of the operator to integrate the instrument readings into a correct diagnosis. The risk of a late or inappropriate response is such that it has been judged better to invoke safety actions and accept the outcome of lost production.

Any delays in procedure-based manual control actions may possibly result in the protection setpoints being reached leading to an automatic reactor trip or other safety system actuation. Even when the operator is successful in arresting a plant transient and averting safety actions, the time required may negatively impact plant operations. The longer a transient is unmitigated, the larger the degree that the plant is subjected to off-normal conditions and the more of a challenge it is to arrest the plant excursion and return to within normal operating parameters. Over time, operator performance is expected to increase through better instrumentation and control, training and protocols, and increases in system reliability.

Digital control systems and sophisticated computer algorithms are now capable of analyzing, diagnosing, and suggesting mitigations to even the most complex and fast-moving situations. Such systems could assist the operators in achieving a more accurate and timely response to component faults and plant transients.

Development of such technology could prove to be enormously beneficial to the currently-operating nuclear plants, as well as the array of new types of nuclear plants that are now being built or proposed. This would result in better management of plant upsets, improved operator performance, and ultimately make a positive impact on the industry's fundamental objectives in the areas of nuclear safety,

production, and cost management. In this report we explore how operators could be assisted by a sophisticated plant monitoring and diagnosis system.



## **2. Computerized Operator Support Systems**

### **2.1 Concept**

Situational awareness is critical to the safe operation of nuclear power plants (NPPs). It requires an accurate understanding of the current plant state and operating configuration, the intricacies of the plant process and control systems, the physics of the plant processes (nuclear, thermal, fluid, and electrical), and the current operating margins with respect to safety and regulatory limits. Today, this enormous amount of information has to be mentally integrated by the operators to arrive at an accurate understanding of how the plant is operating and where it is headed. This is a daunting task for even the most experienced operators and could become a significant concern in the future as a wave of new operators replace the aging nuclear workforce.

As more and more plant information becomes available in digital form, it will be possible to provide operators with advanced information systems that aid in assessing the current plant status, safety margins, and deviations from expected operations. Further, through advanced simulation techniques, it will be possible to predict where the plant is going operationally and how long the operators have to intercede in undesirable plant trends. Finally, the technology can recommend to an operator selected actions that can mitigate undesirable plant events and trends and return the plant to a safe operating condition with the least amount of upset possible.

A computerized operator support system (COSS) is a collection of capabilities to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. They generally have the following features:

- Monitoring a process to detect off-normal conditions
- Diagnosis of plant faults
- Prediction of future plant states
- Recommendation of mitigation alternatives
- Decision support in selecting mitigation actions.

Another common term for this type of technology is “operator advisory system.” This term is generally synonymous with the concept of COSS for the purposes of this project. A number of other similar terms are sometimes used to convey the same concept, such as an “operator assistant”. Other concepts like “recommender systems” are well established in industry and research but represent only a portion of the multifaceted functionality of a COSS.

However, as a class of related technologies, an important distinction to be noted is that they assist human operator as opposed to serving as an extension of the control system. In that regard, the reasoning of the system must be transparent and familiar to the operator, and must operate on a time-scale that allows the operator to interact with the system, as opposed to the much-faster operating speed of an automatic control system.

### **2.2 Relevant COSS Examples**

COSS development has been underway since at least the 1980s in a number of safety-critical applications and has gained widespread acceptance in certain fields, particularly aviation. The following are some notable examples of the use of this technology.

### **2.2.1 Early German Nuclear Plant COSS**

A very advanced concept for a COSS was proposed for certain German nuclear plants in the mid-1980s as described in a paper by W. E. Büttner titled “Advanced Computerized Operator Support Systems in the FRG” [2]. The motivation for the system was to address the burden on operators in dealing with the thousands of control modules and indications in the overall design on a nuclear plant, and to assist them in both normal operations and accident conditions. The tasks of the system are described as:

- Log and record disturbances and accidents
- Reduce the information load and present only essential alarms and messages
- Improve signal supervision and verification
- Enable a fast survey of the plant status (especially in case of accidents) and of the character and location of a disturbance
- Carry out automatic diagnosis of disturbances
- Compute process parameters that cannot be measured directly
- Support operators as they follow procedures in the operating model

This is a remarkable set of objectives, particularly in view of the state of computer technology at the time. In fact, it is a very close parallel to the objectives of this project. It was recognized that a test phase was needed in order to prove that both the new and existing control room technology would work well together, and that these tests must be run on a plant simulator with actual operators participating. Information was not available on the results of these tests or any subsequent implementation in the German nuclear plants.

### **2.2.2 Halden Reactor Project’s Operator Assistant**

A conceptual framework for an Operator Assistant support tool was described in a white paper by the OECD Halden Reactor Project (HRP) in 2012, which was based on experience from the development of various operator support systems using on-line simulation models [3]. It addressed the benefits of using on-line simulation and advanced visualization techniques for assessment of historical data and predictive analysis. The scope of the concept was the full range of operations—normal, disturbance, and accident—as described below.

- For normal operations, provide assistance to the operators when drift in plant parameters occur and give operators early warning before operational limits are challenged. This employs various technologies in surveillance, signal validation, condition monitoring, and fault detection.
- For disturbances, assist the operators in bringing the plant back to a safe state. This involves the use of technologies for computerized procedures, alarm processing, and diagnosis of abnormal situations.
- For accidents, provide prognoses and provide support for alternative actions. This involves the use of critical function monitoring and a HRP-developed computerized accident management support system.

A number of underlying methods and techniques have been applied and combined in various ways to provide these capabilities, such as:

- Data processing and signal pre-processing/conditioning
- Empirical methods for signal validation and diagnosis

- Logic processing for alarm handling and fault diagnosis
- First-principle process simulation of reactor core behavior and turbine cycle monitoring
- Accident simulations
- Risk monitoring based on probabilistic safety analysis (PSA)
- Innovative human system interfaces (HSIs) for visualizing complex systems behavior including 3D, virtual reality and augmented reality.

This work by HRP represents an important step in the development of COSS technology for advanced control rooms for nuclear power plants and builds on a number of important technology products and prototypes that have been proven through individual research projects and trial implementations.

### **2.2.3 Eascon Operator Advisory System**

An operator advisory system has been implemented at an Integrated Gasification Combined Cycle (IGCC) power plant in Sicily, operated by Isab Energy Company on behalf of ERG Power & Gas [4]. This is a complex made up of 20 power units. The system was installed by Eascon, a large Italian engineering company known for innovation in process automation. Eascon has implemented the system in a number of other process and power plants in several other countries.

The system acquires and integrates information from field instruments, recognizes the current plant conditions, and then gives the operators the appropriate recommendations in order to handle any possible scenarios in the most safe and efficient way. The system provides assistance to operators for:

- Start-up, Shut-down and Emergency Operation
- Abnormal Situation Management
- Normal Operation
- Operator Training with off-line Operator Advisory System
- Generation of Standard Operation Procedures (SOP)

Benefits have been demonstrated in the following areas:

- Improvement of operator skills through continuous training both in on-line and off-line mode
- Sharing of technical and operating know-how between expert and young operators
- Standardization of the operators protocols
- Standard Operating Procedures updating

It is important to note that this COSS technology has been implemented in a number of process and power plants in various countries and found to be cost-effective in assisting plant operators with both normal and off-normal operations. It is significant that these types of operations, that are typically cost-driven, have invested in COSS technology as a means of improving the success of day-to-day operations and minimizing the probability and consequences of plant operational disturbances.

### **2.2.4 Traffic Collision Avoidance System (TCAS)**

As an example from the aviation industry, the use of Traffic Collision Avoidance Systems (TCAS) is now mandated for U.S. passenger-carrying aircraft (30 seats or greater) [5]. The first version of this (TCAS I) provided the pilot with only traffic advisories (TAs), meaning information on the altitudes and flight paths of other aircraft in the immediate vicinity. The current version (TCAS II) provides both traffic advisories and resolution advisories (RAs). An RA is a recommendation on control actions to change

course and thereby avoid the pending collision. For example, a RA might be to climb at a certain rate (feet/minute). When both aircraft involved in a potential collision are equipped with TCAS II, the two TCAS units communicate with each other and coordinate their RAs such that complementary RAs are selected. In other words, the units ensure that a secondary collision path is not created.

TCAS has the form of a COSS in that it:

- Receives data from the operating environment,
- Monitors for potential safety issues
- Provides routine updates on safety status
- Detects and diagnoses a critical safety issue
- Provides recommendations to the operator (pilot) to avert the situation
- Monitors for successful resolution.

TCAS has undergone extensive evaluation studies to fine tune the collision avoidance algorithms to reduce nuisance alerts. It was recognized that a high rate of unnecessary alarms would undermine the credibility of the system with the flight crews. Over time, the technology has improved to where most countries have now mandated the use of TCAS for their national airlines.

Also of interest has been the way manufacturers of avionics have integrated the TCAS into the digital instrumentation that is typical on newer aircraft with “glass cockpits.” Rather than just rely on text-based messages, the recommended control actions are superimposed on key flight instruments (such as the attitude indicator and the vertical speed indicator) using a color scheme to assist the pilot’s immediate comprehension of what evasive maneuvers are needed. Again, these are recommendations for which the pilot can opt not to take, but the proven reliability of the technology along with the sophisticated presentation of the recommendations have driven a widespread acceptance of the use of TCAS among pilots and aviation regulatory authorities. This stands out as a real success story of an operator advisory system being a proven complement to a human operator.

### **2.2.5 Terrain Avoidance and Warning System (TAWS)**

A similar example from aviation is a Terrain Avoidance and Warning System (TAWS) that alerts a pilot to what the FAA terms “controlled flight into terrain” [6]. This is when an airplane that is completely airworthy is unintentionally flown into terrain due to lack of awareness by the flight crew. Sometimes these situations are due to adverse weather or darkness, and other times they are due to the pilot becoming distracted.

TAWS typically use a moving map that is displayed on a dedicated instrument or superimposed on general-purpose flight panel displays which depict other information, such as flight path, landmarks, weather, other nearby aircraft (from TCAS), etc. They typically use GPS inputs to know the position of the aircraft and altimeter inputs to know the altitude of the aircraft. They have on-board detailed terrain databases that can be correlated to the position and altitude of the aircraft. The terrain databases are maintained up to date, so that in addition to the natural topography, they contain the latest information on man-made features such as radio antennae and tall structures.

These systems use color to indicate the proximity to terrain features and use text and aural alerts to warn the pilots. A typical sensitivity setting for terrain below the aircraft would be to color the terrain on the map yellow if it is within 1000 feet of the aircraft and red if it is within 500 feet. Using a “look ahead” feature to avoid level flight into rising terrain, the TAWS would calculate the time to impact based on location and ground speed, typically issuing an aural alert one minute before impact.

The system passively monitors the flight path and “pushes” alerts to the pilot when needed rather than requiring the pilot to make any request of the system. In other words, it does not create any distraction in the cockpit other than when urgent action is needed. Some of the situations for which the TAWS provides alerts are:

- Excessive rate of descent
- Excessive closure rate to terrain
- Altitude loss after takeoff
- Negative climb rate
- Flight into terrain when not in landing configuration
- Excessive downward deviation from glide slope
- Premature descent
- Terrain along future portions of the intended flight route.

These systems have the features of a COSS in the sense they:

- Passively gather flight information (e.g., position, altitude, flight path)
- Process this information using models of terrain, glide slopes, etc.
- Provide routine status to the pilot through the flight displays
- Provide text-based and aural alerts (e.g., “Caution, Terrain!”)
- Provide aural recommended actions (e.g., “Pull Up!”)

The use of TAWS has greatly improved flight safety across the aviation spectrum, from high performance commercial and military aircraft down to small general aviation aircraft. It is required by the Federal Aviation Administration (FAA) on most passenger-carrying aircraft.

As in the case of the TCAS, TAWS serves as an excellent example of where an operator advisory system, in this case for pilots, greatly enhances situational awareness and provides reliable recommendations during time-critical safety situations.

## **2.3 Relevance to NPP Control Room Operator Performance**

The success of the commercial nuclear industry is founded on the principle of pursuing continuous improvement. This is particularly true in the concept of operational focus. Yet technology for control room operators is essentially unchanged over the history of the commercial nuclear industry, mainly because the technology in the control room is essentially unchanged in terms of its capabilities, with a few specific exceptions such as what was implemented in response to the Three Mile Island accident (e.g., the Safety Parameter Display System).

The control room operator remains in the role of integrating all of the information that comes into the control room. It is true that a perfect understanding of changing plant conditions is not relied upon to manage plant upsets under the concept of symptom-based abnormal operating procedures. Rather, operators are required to match indications and alarms to procedure entry conditions, and then allow the procedures to guide the control room to the correct event diagnosis and required control actions. However, operators have to be sure that they are in the right procedures for the plant conditions, and this requires correct situational awareness.

In 2010, the Institute for Nuclear Power Operations (INPO) issued *Significant Operating Experience Report (SOER) 10-02 Engaged, Thinking Organization* [7] which described a number of safety lapses that

had recently occurred in the industry and highlighted a number of organizational shortcomings associated with these events. Among these were:

- Lack of monitoring and cross-checking of critical indicators
- Operators and shift managers distracted by ongoing control room activities and failing to maintain oversight
- Weaknesses in worker knowledge, and more specifically in understanding the bases of procedures, systems and components, and integrated plant operations.
- Low risk awareness, particularly in off-normal plant conditions.

The SOER also contained a number of recommendations to improve safety performance at the leader, supervisor, and individual levels. These included re-emphasizing a number of important principles that are foundational to the industry's safety culture including:

- Oversight of plant operations and control room crew performance, particularly control room monitoring of plant parameters
- Managing control room distractions
- Use of significant operating experience
- Use of error reduction tools
- Consideration of most-likely undesired consequences of actions
- Improved worker knowledge.

Basically, the SOER recommendations relied on improvements in management systems and human performance. It did not introduce any new concepts but rather reinforced current performance expectations. However, it is reasonable to think that the safety lapses that led to the SOER were not beyond the scope of the current performance expectations, and had these expectations been fully met, many if not all of these situations would likely have been avoided, or at least greatly reduced in significance. The industry has certainly benefitted from the response to SOER 10-2 in reinforcing these expectations, and no doubt additional safety events have been avoided.

However, the ongoing problem is that the industry continues to struggle with the consistent application of these fundamental performance expectations because they rely on human performance, which is always subject to variation. The industry operating record over the recent past indicates that the trend in performance is, at best, flat, and that the means of achieving continuous improvement in plant operations has been elusive.

It is therefore reasonable to consider additional means of achieving the level of operator performance that is desired. There is no question that technology is underutilized for this purpose. In contrast, other industry sectors have amply demonstrated that technology in the form of a COSS, as an operator advisory system, can enhance operator human performance while maintaining the role and responsibility of the licensed operator as the independent and ultimate decision-maker.

The nuclear industry has long understood the potential value of COSS and has pursued various forms of it as far back as the early-1980s. One notable contribution was by the Electric Power Research Institute (EPRI), working with Westinghouse Electric Corporation and other industry partners, in developing a report entitled *Disturbance Analysis and Surveillance System (DASS) Scoping and Feasibility Study*, published in 1982. [8] The proposed DASS envisioned 14 computerized functions that would assist an

operator in managing disturbances that threatened nuclear safety and plant availability. Some of the notable functions were:

- Plant data indicator verification
- Disturbance detection
- Disturbance cause determination
- Disturbance propagation prediction
- Best corrective action determination
- Procedure monitoring

Another important development in COSS was the International Atomic Energy Agency (IAEA) report entitled *Development and Implementation of Computerized Operator Support Systems in Nuclear Installations*. [9] This is a valuable reference document on the concept and practical considerations for a COSS and is just as relevant today as when it was published in 1994. Topics include:

- Concept of COSS for a nuclear installation
- Operational requirements
- Design methodology
- Verification and Validation
- Implementation
- Licensing Considerations

This IAEA report indicates that nuclear industry leaders at the time well-understood the importance and benefits of COSS technology in improving operator performance as a continuation of the application of control room human factors engineering to improve operational safety.

However, progress in this direction, at least in the U.S., was apparently overcome by the more prominent focus on improving operator performance through control room protocols and the establishment of defensive barriers to prevent errors from resulting in events. And, in fairness, the state of digital technology was, at the time, marginal for being able to accomplish the objectives of a highly capable COSS.

It is now clear that there is a role for both. The challenge is to see how advanced operator advisory systems could complement the human performance protocols for control room operators. The state of digital technology today is such that a capable and well-designed COSS is indeed feasible, as already demonstrated in other industry sectors, notably aviation.

This project proposes a general model for a control room COSS that addresses the control room operator performance challenges that have led to undesirable events. Further, a prototype COSS has been developed to enable the study of this technology in order to refine the concept, determine the appropriate system objectives and requirements, resolve all human factors issues with the technology, and ultimately validate the COSS concept for commercial product development leading to use in a nuclear power plant control room.



### **3. CVCS COSS Conceptual Model for Fault Management**

#### **3.1 General Concept**

This particular concept of a COSS is framed as an “operator advisory system”, assisting operators in diagnosing and mitigating certain plant events that, unless addressed in a timely manner, would likely result in a plant transient or reactor trip. This is most often the domain of the plant’s Abnormal Operating Procedures (AOPs). These procedures are symptom-based with one or more entry conditions that have to be recognized by the operator. These would include alarm conditions, equipment faults, and plant parameter trends.

There can be time-pressure associated with these plant upsets to recognize the AOP entry conditions, enter the appropriate procedure, and then work through the diagnostic steps until the correct mitigation actions are taken to resolve the situation. In some cases, the underlying fault is not really identified at a component level, but instead the consequences of the fault are managed. For example, there might be a leak on the reactor coolant system that is identified by its symptoms (high containment humidity, high containment sump level, etc.) but the exact location of the leak cannot be determined, other than it is inside containment. However, the AOPs are structured such that the mitigation actions are effective without knowing the exact location of the leak other than determining the general location.

In all of this, the operator is the point of integration of all control room information and has to use what is termed “operator fundamental knowledge” to ensure that indeed the control room is applying the correct procedure for the plant upset. Operators are trained to use a number of human performance enhancement techniques to correctly assess the situation, such as using a questioning attitude and validating all information. In addition, there are a number of other techniques used in the control room at a crew level, such as pre-job briefs, time-outs, repeat-back communications, independent verifications, etc. While all this has proven to be very helpful and necessary, it adds to the mental workload and increases the time delay in responding to the actual plant upset.

The control room crew typically follows a general pattern in reacting to a plant fault as follows.

- Detection – recognizing the symptoms of a plant fault
- Validation – determining that the symptoms are the result of a real plant fault and not a sensor failure
- Diagnosis – determining the specific plant fault
- Mitigation – either correcting or isolating the plant fault such that it is no longer a threat to plant operations or nuclear safety
- Monitoring – monitoring the symptoms of the plant fault to ensure that the mitigation has been successful
- Recovery – restoring the plant to the pre-fault conditions.

Again, the control room procedures, particularly the AOPs, assist the operator with these tasks provided that the correct procedures have been entered. However, the procedures are not specific in certain areas and rely on the operators to perform certain knowledge-based functions, such as estimating the size of a leak based on available plant indication. For example, a leak size can be roughly determined by the per cent decrease in a tank level from the known steady-state value.



Operators are exceptionally good at performing these tasks, but the high workload associated with certain plant events creates an environment that adds to the likelihood that the operator will commit errors that compound the original fault and impact the plant more so than would otherwise have occurred.

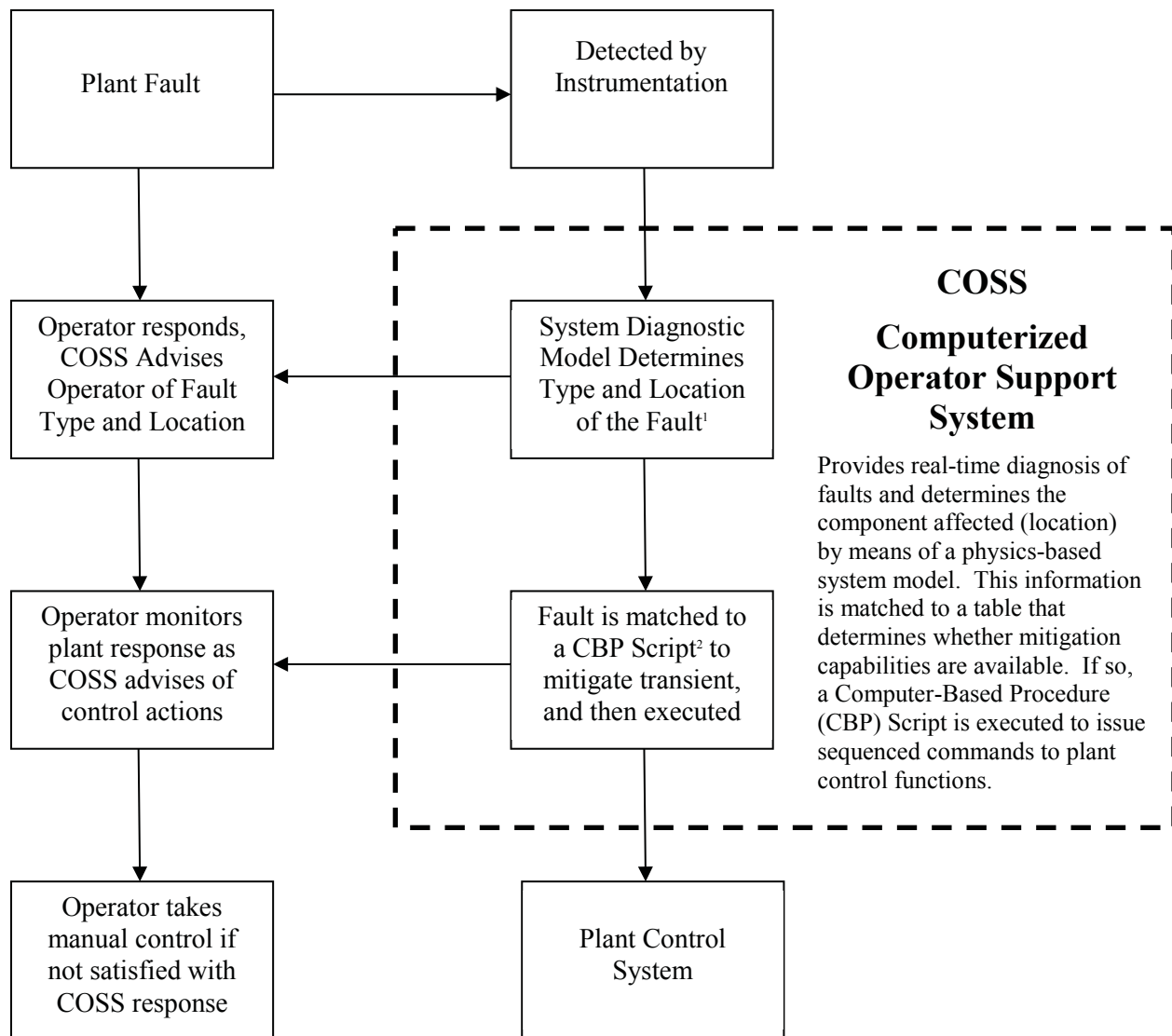
### 3.1.1 Overview of COSS Features

A well designed COSS can assist an operator at each stage of the fault response sequence to reduce workload and confirm important information. Table 1 illustrates the functions of a COSS as it assists an operator in responding to a COSS.

**Table 1. COSS Functions.**

<b><u>Step</u></b>	<b><u>COSS Function</u></b>
Detection:	Detect a plant anomaly before an operator would notice it. This could actually be in the noise-level of the instrument signal and long before it would be noticeable as a parameter trend or reach an alarm set point.
Validation:	Determine whether an apparent fault is real or caused by sensor failure by cross-checking related plant parameters and calculating whether the sensor in question is reading correctly.
Diagnosis:	Determine what type of fault would explain the values of the related sensors once they had been validated as reading correctly. This is based on using various means to model the expected behavior of a plant system. This could also include physics-based models that perform calculations for mass and energy balances to accurately determine where the fault condition must be. In other words, the plant system model is compared to the validated readings of the actual plant to precisely locate the point of deviation from expected behavior. The COSS could provide a graphical depiction of the fault to the operator for quick comprehension of the nature of the situation.
Mitigation:	Determine if there is a successful mitigation for the plant fault other than putting the plant in a safe condition (e.g., manual reactor trip prior to automatic protective actions). If so, the appropriate procedure could be displayed for the control room crew to begin actions. The COSS either allows the operator to execute the procedure in the normal manner, time permitting, or directly executes the relevant sections of the procedure as a script.
Monitoring:	Determine whether the plant parameters indicating the apparent fault are trending towards values that indicate that the fault has been mitigated, and inform the operator that the mitigation actions are being effective.
Recovery:	Direct the operator to the appropriate recovery procedures based on the extent of the plant upset due to the fault. An example would be determining the volume of fluid lost during a leak to know the magnitude of the make-up requirement. Another example would be determining the time available to remain in an emergency plant configuration, such as relying on batteries until normal power is restored.

These concepts are developed in more detail in the following sections. The role of the COSS interfacing with the human operator and plant instrumentation and control is depicted in Figure 1.



1. Diagnostic Model developed in PRODIAG
2. CBP Script developed in LWRSP Computer-Based Procedures Pilot Project

**Figure 1 COSS Interface with operators and plant systems**

### **3.1.2 Observance of Licensed Operator Duties and Responsibilities**

It is important to note that a COSS is not an extension of the control system, but rather an advisory capability for the operator, to be used as the operator determines to be prudent and useful. While the COSS will passively collect data as a background function, at no time will it interact with the plant other than as directed by an operator.

It is well-recognized that the COSS cannot encroach on the duties and responsibilities of a licensed operator and therefore certain protocols must be upheld at all times.

- No plant control actions would be taken by the COSS.
- COSS recommended control actions would be executed either by manual operator actions or through an approved computer-based procedure system with soft-control capability, and then only as commanded by the operator, including the execution of automated sequences of steps.
- The logic of the COSS in advising in the various steps of the fault response process must be assessable and transparent to the operator.
- The operator is free to disregard or turn-off the COSS at any time, and then address the plant fault using traditional control room protocols.
- The operator can take manual control of any automated procedure sequences at any time during the execution. Likewise, the operator can reinitiate automated sequences at any time.

The effect of a COSS on control room human factors and operator protocols will be the subject of extensive research and development in the future. It is recognized that some COSS concepts would challenge some aspects of the present expectations for control room “conduct of operations” in the current Light Water Reactor fleet. Yet, these types of systems have been successfully integrated into other safety-critical operations, such as the role of flight management systems and flight directors in modern aircraft cockpits. Future work will include the application of sound principles for determining how to do this, as well as validation studies in full-scope plant simulators using experienced operators.

### 3.2 Sensor Validation

Sensors are important nuclear power plant components and are required to provide accurate and reliable process variable measurements to ensure maximum availability, capacity factor, and power output. Their use in harsh environments as found in nuclear plants, however, results in structural deterioration with time, eventually causing sensor readings to become unreliable. Sensors that fail have associated safety and operational consequences. Operator actions may be inappropriate if based on a faulty reading and can result in unnecessary thermal cycling of equipment. Safety systems may be inadvertently actuated resulting in lost availability. Post-accident plant status may be incorrectly assessed. Thus, plant reliability and safety stand to benefit by validating sensor readings so that degraded sensors are identified.

In addition to plant performance issues associated with failing sensors, the introduction of advanced computer-based operator aids for increasing operator awareness to improve plant operation requires quality sensor data. There must be a high degree of confidence that a reading accurately represents the underlying physical process-variable value. To do so, the data must be tested for correctness, typically quantified as a maximum permissible error, and failing sensors identified.

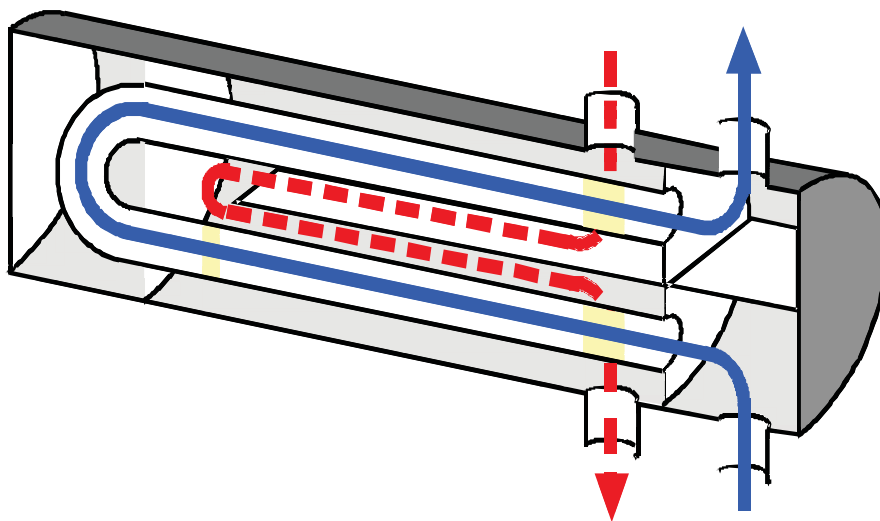
The current industry practice for detecting failing sensors is *ad hoc*, time consuming, and presents a significant mental challenge to the operator. The operator must scan thousands of sensor readings and correlate these with his own mental model for the underlying physical processes. Thus improved methods are needed to automate sensor validation and to do it more reliably than an operator.

The sensor validation technology, Algorithm for Transient Multivariable Sensor Estimation (AFTR-MSET), has been selected for assessment and demonstration on the full-plant simulator [10]. This choice was based on several criteria judged to be important by the authors from their first-hand experience with validation algorithms and their familiarity with the sensor validation literature. The over-arching issue relates to a high-false alarm rate among the many different algorithms that presently exist. The technology selected for assessment treats the root causes of false alarms, which include 1) the inability of many

algorithms to perform extrapolation or to operate with data where plant dynamics have been excited and 2) the absence of guidelines for how the measurement vector should be composed or for what is an appropriate set of training data to ensure the physical behavior of the system is adequately captured.

The AFTR-MSET method starts with a representation of the conservation laws for the physical system written as a set of ordinary-differential equations. This model does not need to be known in detail, but an understanding of its general structure is needed for developing a robust data-driven model. Conditions that the training data must satisfy are identified to ensure a reliable and robust data-driven model. Sensor fault detection and identification in AFTR-MSET is based on computing the residual-error vector. The correct error vector is found as the residual, which produces the best fit of the error-free estimate of the observation to the column space of model basis vectors. The residual, which localizes errors to the “bad” sensors, is found by a search in the space of all possible error vectors.

The performance of AFTR-MSET for detecting and identifying failing sensors has already been assessed in standalone applications. This involved simulating the thermal-hydraulic behavior of individual plant components such as heat exchanger and coolant pipes in response to changing forcing functions. The algorithms are housed in a “test stand” environment that facilitates running different transient and injecting signals into sensor models to simulate failure. One application involved the instrumented regenerative heat exchanger shown in Figure 2 and the exercising of the algorithms through the test stand. A screen shot of a GUI on the test stand appears Figure 3.



**Figure 2 Regenerative heat exchanger.**

Preparations are in place to advance the sensor validation AFTR-MSET technology to the next level of performance testing. Whole-plant simulator trials will provide for additional conditions not achievable under the existing test-stand environment. It will provide for integration of the algorithms across multiple components, rather than single components as has been the case to date. It will provide for a human factors assessment of how operators might interact with the technology. A full-scale simulator replicates the physical space, data display, and communications technologies found in an advanced power plant, and thus represents a realistic environment for assessing operator use. Whole-plant simulator trials will also provide a forum for demonstration to utilities. All such features of the whole-plant simulator environment will serve to guide the development of AFTR-MSET for deployment in existing and future plants.

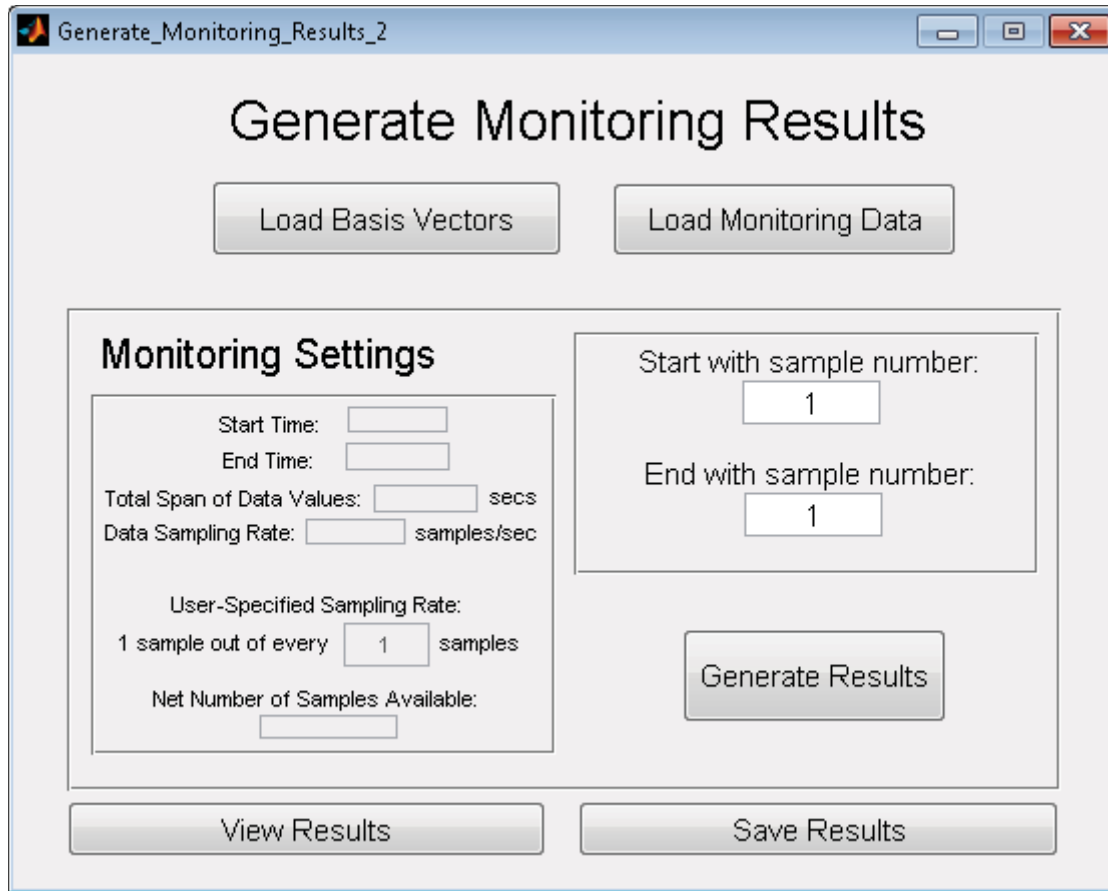


Figure 3 Screenshot from the AFTR-MSET test stand.

### 3.3 Fault Detection and Diagnosis

An equipment fault involves a redirection of mass, energy, and momentum (MEM) as a consequence of a physical change in the system from its normal state. In general then to diagnose a fault a reasoning process is needed that can relate observed changes in process variables due to redirection of MEM back to the physical change in the system that corresponds to the fault. This differs from sensor fault diagnosis, which does not require such complex reasoning.

Presently the operator is provided with no advanced technology aids for performing fault diagnosis. He is hampered by the magnitude of the mental task needed to correlate trends among a myriad of sensor readings to deduce the identity of the fault. In particular he must reason how different faults would play out through the conservation laws and give rise to trends in sensor readings with time. The identity of the fault will be arrived at by correctly matching trends based on the conservation laws with observed sensor trends. This process as is currently performed manually by the operator is time consuming, approximate, and prone to error.

Implementing this reasoning process on a machine which serves as an aid to the operator has potential advantages. The machine is not subject to the limitations of an operator who tires with time or can be distracted. There is fundamentally no limit to the workload the machine can handle. The machine can reason quantitatively to evaluate trends versus the less precise and more limited quantitative reasoning an

operator is capable of. The machine offers the potential for a timelier, more sensitive, and more reliable diagnosis of equipment faults.

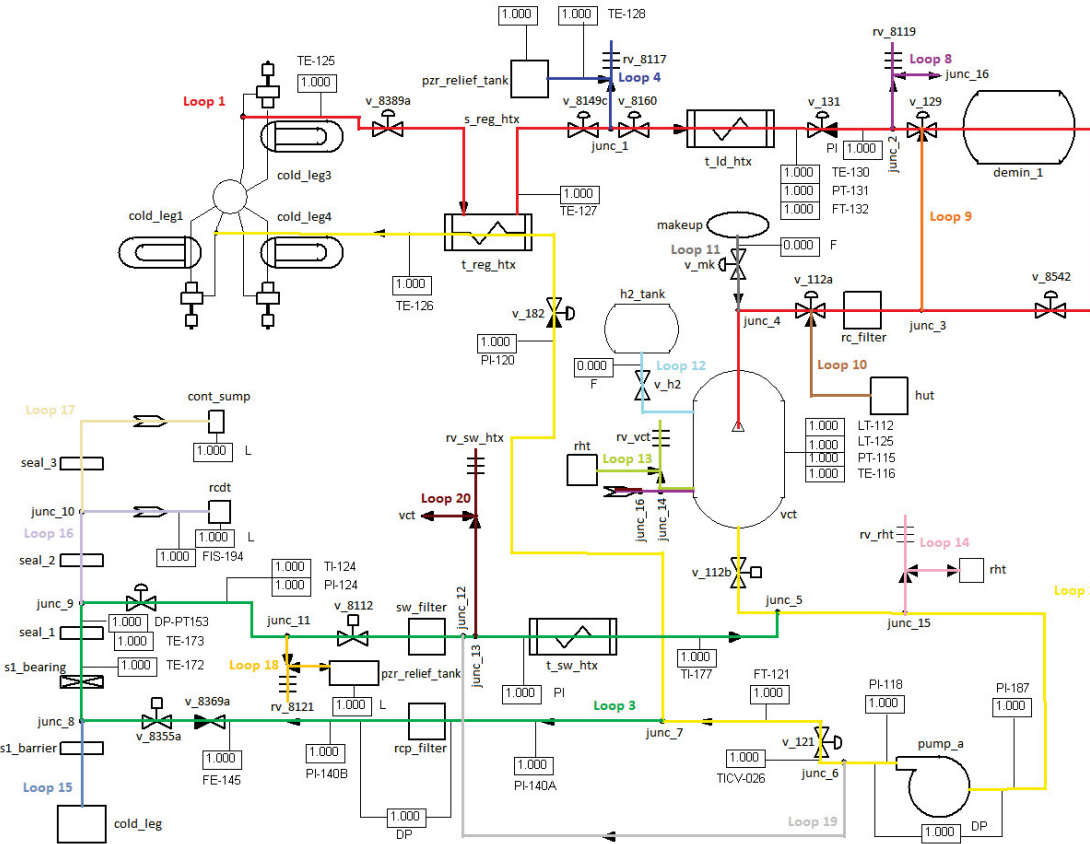
Important considerations in the development of a reasoning engine are the following. First, it is important that an anomalous sensor reading resulting from a component operating outside its normal range as a result of an equipment fault not be mistaken for a failed sensor. The method of the previous section provides a capability to ensure this. Second, the conservation laws and sensor readings should act as constraints during the process of diagnosing a fault. That is, the ultimate diagnosis must be consistent with the sensor readings and the physics of the faulted plant. Third, the reasoning process should not be dependent on furnishing *a priori* a list of candidate faults to be processed by elimination. That is, the engine should have reasoning powers that allow it to deal with unforeseen faults, i.e., those that might be inadvertently left off of a pre-prepared list of possible faults. Fourth, the reasoning engine should be structured so that plant specific input that must be provided to the algorithm is limited to process instrumentation diagram information. That is, the reasoning rules and their processing are formulated in a way that does not require a custom re-write for each new plant. Finally, the conservation laws should be formulated in a way that avoids explicit modeling of rate processes. That is, there should be no requirement for supplying engineering parameters (such as heat transfer coefficients, friction factors, etc.) to the engine.

The process diagnostics (PRODIAG) method for automated diagnosis of faults in nuclear power plants (NPP) [11] was developed with the above considerations in mind. Data from plant sensors are sampled periodically and trends are compared against the steady-state condition to determine if an anomaly exists. If an anomaly is detected, the code attempts to identify the cause through a reasoning process that involves rules that relate faults to sensor trends combined with knowledge of how plant components are connected.

In PRODIAG the most basic function of components in thermal-hydraulic (TH) processes are recognized as sources or sinks of mass, energy, and momentum (MEM). Once components are classified as sources or sinks of these three functions, detecting imbalances in the conservation of MEM can identify their malfunction. The advantage of this function-oriented approach stems from the relatively small number of generic types of components (e.g., pump, valve, and heat exchanger) utilized in TH processes and the fact that each component is designed to perform basically one key function. In contrast, there are hundreds or even thousands of possible modes of component failures in nuclear power plant processes.

PRODIAG's reasoning is based on qualitative physics where a small number of qualitative values, such as increasing, decreasing, and unchanging trends, are used to represent the values of continuous real-valued variables. Qualitative reasoning approximates the back-of-the-envelope calculations that analysts use to confirm, semi-quantitatively, certain general numerical features of a transient response. By taking a qualitative reasoning approach, generality is gained. For example, the trend information of a flow signal can be used for diagnosis without knowledge of the exact numerical value of the flow signal and independent of the process.

The performance of PRODIAG for diagnosing equipment faults has been assessed in standalone applications. This has involved simulating the thermal-hydraulic behavior of the Chemical and Volume Control Systems (CVCS) in a Pressurized Water Reactor (PWR) in response to changing forcing functions. The PRODIAG algorithm is run on a platform that concurrently supports execution of the CVCS model. A screen shot of an HSI is shown in Figure 4. Currently, the performance of PRODIAG is being evaluated by introducing equipment faults into the CVCS and then examining the diagnosis correctness as a function of number, location, and types of sensors, severity of the fault, and magnitude of process noise.



**Figure 4 Screenshot of a simplified PRODIAG representation of a CVCS.**

Preparations are in place to advance the PRODIAG fault diagnosis code to the next level of performance testing. Whole-plant simulator trials will provide for additional conditions not achievable under the existing test-stand environment. It will provide for integration of the algorithms across multiple components rather than single components as has been the case to date. It will provide for a human factors assessment of how operators might interact with the technology as the full-scale simulator replicates the physical space and data display and communications technologies found in an advanced power plant and thus represents realistic environment for assessing operator use. Whole-plant simulator trials will also provide a forum for demonstration to utilities. All such features of the whole-plant simulator environment will serve to guide the development of PRODIAG for deployment in existing and future plants.

### 3.4 Fault Mitigation

Once the fault has been diagnosed, the fault must be mitigated in one way or another. Obviously, the most desirable way causes the least upset to the plant, if such an option is available. In some cases, there is no alternative but to trip the reactor and address any safety challenges through the Emergency Operations Procedures (EOPs).

Fault mitigation as part of a COSS starts with matching the fault to a table of validated mitigation strategies. In turn, these strategies are cross-referenced to procedures that direct the control room operators to take the needed actions to mitigate the fault. To be clear, these are the same procedures that



would be used in a manual mode if the COSS was not operative. However, in this case, the benefit to the operator is the assistance in matching the diagnosed fault to the correct procedure and having the procedure automatically displayed on the operator's console. The operator must independently verify that the right procedure has been referenced.

The COSS will continue to update information about the fault and plant response to the operator. This will include estimated times to alarms and automatic protective actions, as well as remaining time for the completion of Emergency Plan requirements and Nuclear Regulatory Commission (NRC) reporting requirements.

The COSS will use a computer-based procedure (CBP) system to display the procedure content and to provide soft controls for operator control actions through the procedures. This will be displayed on a second operator display.

The CBP will be compliant with IEEE 1786-2011, *IEEE Guide for Human Factors Application of Computerized Operating Procedure Systems (COPS) for Nuclear Power Generating Stations and Other Nuclear Facilities* [12]. This is specifically in regard to Type 3 Procedures that use soft controls and the guidance for a sequence of steps that can be automatically executed.

The COSS will enable the operator to execute the procedure with the following options:

- To execute the steps through the control board-mounted devices in a completely manual manner.
- To execute applicable procedure sections one step per command of the operator through the CBP soft controls.
- To execute the applicable procedure sections using automated sequences built into the CBP soft controls. In this case, the operator can interrupt and restart the sequence as desired.

By any of these means, the operator will work through the applicable procedure sections to mitigate the fault and resultant plant upset. These actions will be terminated according to the procedure when the desired result has been achieved.

### **3.5 Monitoring**

The COSS will continue in a monitoring mode throughout the event and continue to update pertinent information. Once the applicable procedure sections have been completed, the COSS will determine whether they have been effective and whether plant conditions have stabilized, depending on the nature of the fault. This information will include actual values of relevant plant parameters along with short-term trend lines. This information will be reported to the operator display in real-time.

The COSS will continue to monitor associated requirements concerning the Emergency Plan and NRC reporting. It will monitor any other time requirements imposed by the procedures, and indicate whether they have been met, whether they have been exceeded, or whether the exit criteria for the requirement has been met.

Special displays for this type of information will be standardized and reviewed for human factors concerns such that there is a consistent and logical presentation of information regardless of the type of plant fault being monitored.

The COSS will continue to monitor the event until redirected by an operator.



### **3.6 Recovery**

The COSS will assist in the recovery from the event as appropriate. This will include providing a list of related off-normal plant parameters affected by the event and displaying their current values, their pre-fault values, and their target values for current operations. The COSS will provide a list of plant procedures needed to return the plant to conditions where plant parameters are restored. For instance, where there had been a fluid leak and a tank was left at a lower level than desired, a procedure would be referenced for returning the tank to its desired level, such as manually running a make-up system.

The desired order of the recovery actions would be suggested by the COSS, but the operator could elect to run them in any desired order, other than where certain sequences must be observed, and again, the COSS would monitor and advise on this.

## 4. Computerized Operator Support System Prototype Development

### 4.1 COSS Design

#### 4.1.1 Design Elements

In order to demonstrate COSS concepts discussed in earlier sections of this report, a functional prototype was developed using a digital control system (DCS) architecture. As noted earlier, the COSS is a composite system that features several distinct yet co-equally important elements. For the purposes of the prototype, four separate facets of the COSS were considered:

- *Digital Alarm System*: The COSS includes advanced alarms that are designed to combine the spatial pattern recognition afforded by traditional annunciator boards with supplemental information to help the operator understand the cause of the information. The COSS digital alarm system provides a trend display for key indicators coupled with multistate colored alarms for warning and alarm states. The alarm trend displays also incorporate a mechanism for showing sensor drift or failure.
- *Computer-Based Procedure (CBP) System*: The COSS also includes a CBP system. The CPB closely mimics the paper-based procedures for abnormal and emergency operations, including the common two-column format with a left hand column for the preferred operator action and a right hand column for response not obtained. The CBP builds on paper-based procedures by providing digital indicators embedded in the procedures and soft controls the operator can activate within the procedures.
- *Piping and Instrumentation Diagram (P&ID)*: The P&ID provides a schematic of key plant components in a system. This display includes visible indicators of key states (e.g., valve position pump energized, or tank level) as well as the actions available to the operator (e.g., open or close valve). The P&ID does not incorporate flow indicators, which are displayed as part of the alarm trends.
- *Recommender System*: The heart of what makes the COSS distinct from advanced DCS displays is the recommender system. The recommender system monitors plant states and provides suggestions to the operator to help diagnose problems and take actions. The recommender system monitors multiple sets of sensor data and can provide early warnings of emerging system faults (e.g., rapidly lowering level) before they are alarmed. The recommender system interacts with the digital alarm system, CBP system, and P&ID displays, directing the operator to relevant information and available actions and procedures.

Note that the initial prototype does not yet include full integration with AFTR-MSET for sensor validation or PRODIAG for fault diagnosis. Functionally, however, these are modeled in the COSS interface. For example, sensor drift is visually indicated in the alarm trend displays. Likewise, fault detection is handled by the recommender system. The alarm trend displays and the recommender system serve as the HSIs for AFTR-MSET and PRODIAG, respectively, and will be enhanced with greater sensor validation and fault diagnosis capabilities in future releases.

The four COSS elements as well as the accompanying HSI are described in further detail in Section 4.3 of this report. Detailed specifications for the COSS can be found in Appendix A.

### 4.1.2 Design Philosophy

The CVCS was selected as the system to model for the prototype, in part because it is modeled in PRODIAG and because it is one of the systems that has been successfully implemented in DCSs as part of control room modernization [13]. Figure 5 illustrates the DCS for a CVCS at a recently modernized NPP. As can be seen, the DCS incorporates elements of a P&ID coupled with digital indications and soft controls. Such a DCS is being used to improve operator control of the CVCS, and it affords some advantages to the operator over its analog antecedents in understanding the dynamic response of the interrelated components. However, the DCS does not explicitly help the operator to diagnose and mitigate upset conditions. The distinct advantage of the various elements of the COSS is that they work together to provide the operator with a comprehensive view of the system and work alongside the operator to evaluate system states.

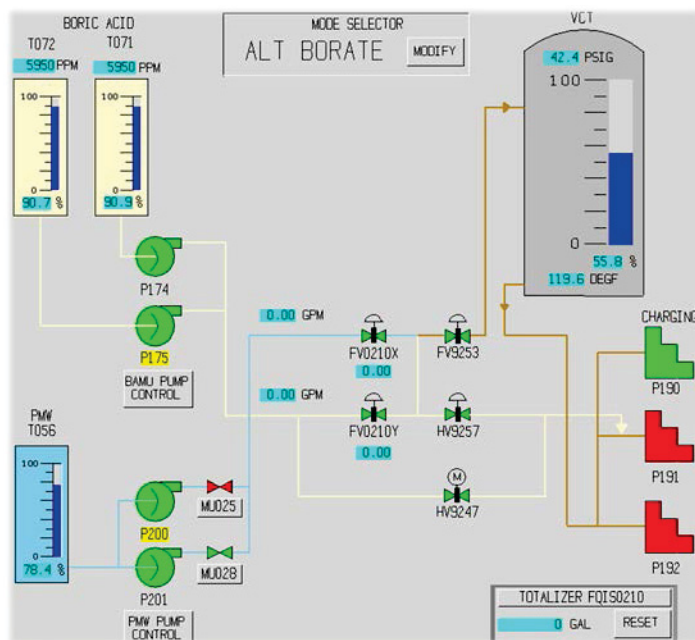


Figure 5 Current DCS for CVCS from a modernized control room at a nuclear power plant.

To realize the benefits of co-equal information sources to the operator, the different parts of the COSS are combined into a single display in the prototype. This display may take the place of a DCS display, but the functionality, particularly the recommender system, exceeds typical DCS implementations. The underlying philosophy of the COSS is that it should both support the tasks the operator must perform and aid him or her in the completion of those tasks whenever possible. Such assistance should be minimally intrusive to manual operations.

The COSS recommender system must not be confused with an automation system. The recommender system does not perform actions automatically or in lieu of the operator. Rather, it monitors overall plant or system activity and advises the reactor operator on the correct course of action, including the correct procedure path to take. Control actions are only performed by the operator, who may do so based on information provided by the recommender system. The reactor operator may also dismiss or ignore recommendations as appropriate.

It is also important to clarify the difference between the COSS recommender system and a CBP system. A recommendation provided by the recommender system is not equivalent to a procedure or procedure step.

The recommender system augments the CBP by directing the operator to the appropriate procedure based on the fault diagnosis. In the prototype version of the CBP, the recommendations are based solely on the procedures, and mitigation actions are not provided other than by the procedures. The recommender system is also not designed to offer step-by-step operational guidance. The recommender system may provide a high-level explanation of what actions the operator needs to take without providing the precise steps required, which are explicated in the CBP. Whereas the recommender system provides top-down guidance, the CBP provides bottom-up instructions to the operator.

### **4.1.3 Design Process**

A team consisting of two human factors psychologists, one software developer, and a process control expert developed the elements of the COSS. The requirements for each system were discussed initially, and preliminary mockups were sketched using a combination of whiteboards, wireframes, and PowerPoint to represent graphically the look and feel of the system. To clarify the functionality of each element, several scenarios relevant to CVCS operations were reviewed, and a storyboard was developed to walk through the flow of the HSI and the functions of the COSS. In deciding between competing design ideas, the team discussed and then voted on particular design elements. Because many of these decisions represented tradeoffs, design decisions were captured for consideration in a future round of COSS designs. Each COSS element was then developed into a software specification (see Appendix A), which was prototyped using Microsoft Windows Presentation Foundation and Microsoft Visual Studio (see Section 4.2 for a brief technical discussion). The completed specifications and prototype were carefully reviewed to ensure a consistent iconography, look and feel, color scheme, navigation, and interactivity. The specifications serve as a general HSI style guide for the COSS.

The prototype represents an initial attempt to put key COSS ideas into practice. The design is far from finalized. The design process includes planned iterative phases of design and evaluation—the design team will implement a prototype version, which is then validated against human factors standards and through operator testing. Walking operators through normal plant and CVCS specific operational scenarios will test the usability and utility of the various elements of the COSS. Performance metrics will be gathered, and operators will be interviewed to document their experiences using the COSS, including any functions that are not found to be helpful and additional features that might improve the COSS. Additionally, other modes of presenting information and controls will be benchmarked against the current design, thereby refining the design for the next version. The findings will be extracted to become design recommendations and will be implemented into the prototype, which will become a final design for the CVCS. The functional CVCS prototype will then become the basis for COSS HSIs in support of additional plant systems.

## **4.2 Technical Considerations**

### **4.2.1 Full Scope Simulation Environment**

The COSS prototype is integrated into the U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) Human Systems Simulation Laboratory (HSSL) located at the INL (see Figure 6). The HSSL is a full-scope, full-scale glass top simulator capable of simulating existing and future nuclear power plant main control rooms. Developing the COSS within the context of the HSSL provides a number of advantages. First, by simulating a physical control board, the location and size of the COSS display can be iteratively evaluated to determine the optimal placement and sizing. The second advantage is scalability. The functionality of the COSS can be expanded to include other systems, such as the turbine control system, which may not be modeled on part-task simulations. Lastly, embedding the COSS

within a high fidelity testing environment enables the demonstration to reflect how the actual technology would be used by providing a realistic environment for operator studies. Consequently, integrating the COSS with the HSSL enhances the validity of the concept as well as the practical applicability.



**Figure 6** A development team member at the helm of the early CVCS COSS prototype embedded in the HSSL.

The full-scope full-scale glass top simulator consists of fifteen virtual panel bays. Each bay contains three 46-inch high definition displays. The displays are arranged in a convex arc relative to the operator. The lower two displays are touch capable allowing users to interact with simulated physical controls in a natural manner. The HSSL simulator is both physically and digitally reconfigurable. This allows it to represent a variety of nuclear simulators running on a variety of simulation platforms, and to arrange the bays to physically map the control rooms of the actual plants.

The COSS DCS is displayed as a picture-in-picture embedded on a vertical display of a simulator bay. This solution mimics the effect of adding a touch panel display to the analog control boards of an actual plant. A primary limitation is the resolution afforded on the displays in the bays. The available resolution for the entire 46-inch display is equivalent to the resolution expected of a 23-inch DCS display at the plant. As such, the HSI was designed to be legible even when scaled to half the resolution found in an actual DCS. Another limitation of embedding the COSS DCS into the context of the control boards is the limited real estate available for displays. Given the large number of indicators and controls on typical NPP control boards, it becomes very difficult to make space available at the boards. While ideally it would be possible to have multiple displays available for the COSS, practically speaking, most plants are challenged even to make room available for the addition of one display on a panel. To realistically emulate this constraint, the COSS DCS is designed to fit on a single display.

#### **4.2.2 Software Development Environment**

This project used the Generic Pressurized Water Reactor (gPWR) simulator as the test bed for the CVCS COSS prototype. The plant simulator was licensed from GSE Systems and the control displays have been tailored to fit the bays using GSE's JADE (Java Application Development Environment) software toolkit. The control boards of the gPWR emulate those of a 1000 MWe 3-loop Westinghouse PWR built in the 1980s. The layout and controls are typical of this vintage of plant.



Another important consideration was the absence of modern digital control systems. The simulator plant model can be interfaced with digital control systems, or other software applications, like Matlab and LabView, through standardized protocols created and maintained by the OPC (Object Linking and Embedding for Process Control) Foundation. The plant model of the gPWR has support for an OPC Client. This allows for the possibility for two-way communication with the plant variables and controls.

Here we decided to implement the COSS prototype with Microsoft Windows Presentation Foundation (WPF). WPF is Microsoft's de facto standard for developing desktop applications and is intrinsically linked to Microsoft's .NET framework. WPF uses a *Code-Behind* model in which the visual look and feel of the interface is segregated from how the visual components are wired together. The Common Language Runtime component of the .NET can produce machine code from several programming languages: Visual Basic, C++, C#, F#, Python (IronPython). WPF also comes pre-equipped with most of the standard and advanced interface modalities one might wish to integrate into a modern DCS. These factors allow for rapid prototyping and an agile software development model. A second compelling reason for using WPF is the robust and well-documented code base. The underlying framework has been heavily optimized for performance, reliability, and security.

Advosol's OPC libraries for .NET were used to link GSE's gPWR to our CVCS/COSS prototype. The primary benefit to building the CVCS/COSS prototype on top of the GSE simulator is that it ensures the validity of the underlying system dynamics and automated control systems. Two-way communication allows the CVCS/COSS to implement soft controls much like a real DCS. While the validity of the system dynamics are assured by the plant model, the process diagnostics are solely mimicked. The scenarios described in this document are initiated from the Plant Simulator Instructor Station. Once initiated, the CVCS/COSS has explicit knowledge of what fault was triggered and can respond appropriately.

## **4.3 COSS Prototype**

### **4.3.1 Display Overview**

The COSS prototype (see Figure 7 for an early prototype and Figure 8 for the most current prototype iteration) is capable of displaying CBPs, a P&ID based on a functional CVCS DCS, and trend alarm panels. The COSS prototype P&ID supports normal plant operations and CVCS specific operations. A large window on the display is reserved for presenting the CBP, P&ID, and detailed trend alarms (see Figure 8 for an annotated screenshot of the COSS display). The P&IDs and trend alarm panels provide diagnostic information to support the operator while he or she interacts with the CBPs. The CBPs are the main method operators can control the CVCS (via embedded soft controls in the procedures), however the operator can make manual adjustments to components by clicking on a component in the P&ID and selecting options within the pop-up menu. An area along the right side of the COSS is dedicated to trend alarms, which allow the operator to have direct view of any associated warnings or alarms at all times while performing all interactions with the COSS. A recommender system provides the operator with warnings and mitigation actions that the operator can select. Selection of a mitigation action automatically displays the desired computer-based procedure relevant to the mitigation action.

The CVCS has both safety and non-safety functions. The CVCS maintains the appropriate reactor coolant chemistry as well as maintains the correct amount of reactor coolant circulating through the primary reactor coolant system. Traditional DCSs offer a simplified representation of the CVCS system, but this limits an operator's ability to monitor the CVCS in the context of the plant at large. CVCS components are also involved with many other plant operations such as safety injection, reactor coolant pump seal

injection, primary makeup water, and auxiliary pressurizer spray valves. The interconnectivity makes it important to monitor these other related systems in addition to the primary CVCS operations. A more capable P&ID interface should afford the operator with the ability to monitor all these interconnected systems, which mandates a more complex P&ID (see Figure 9).

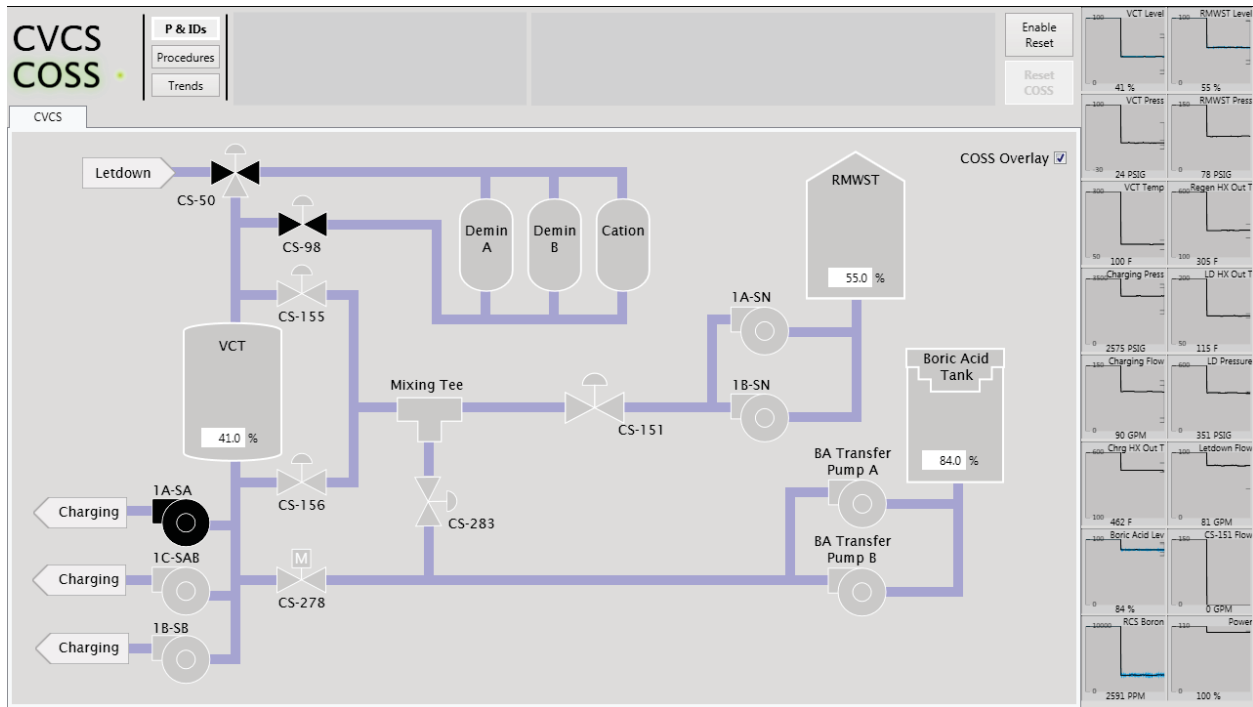


Figure 7 Early prototype of a CVCS COSS display of the P&ID mode during a normal operating state.





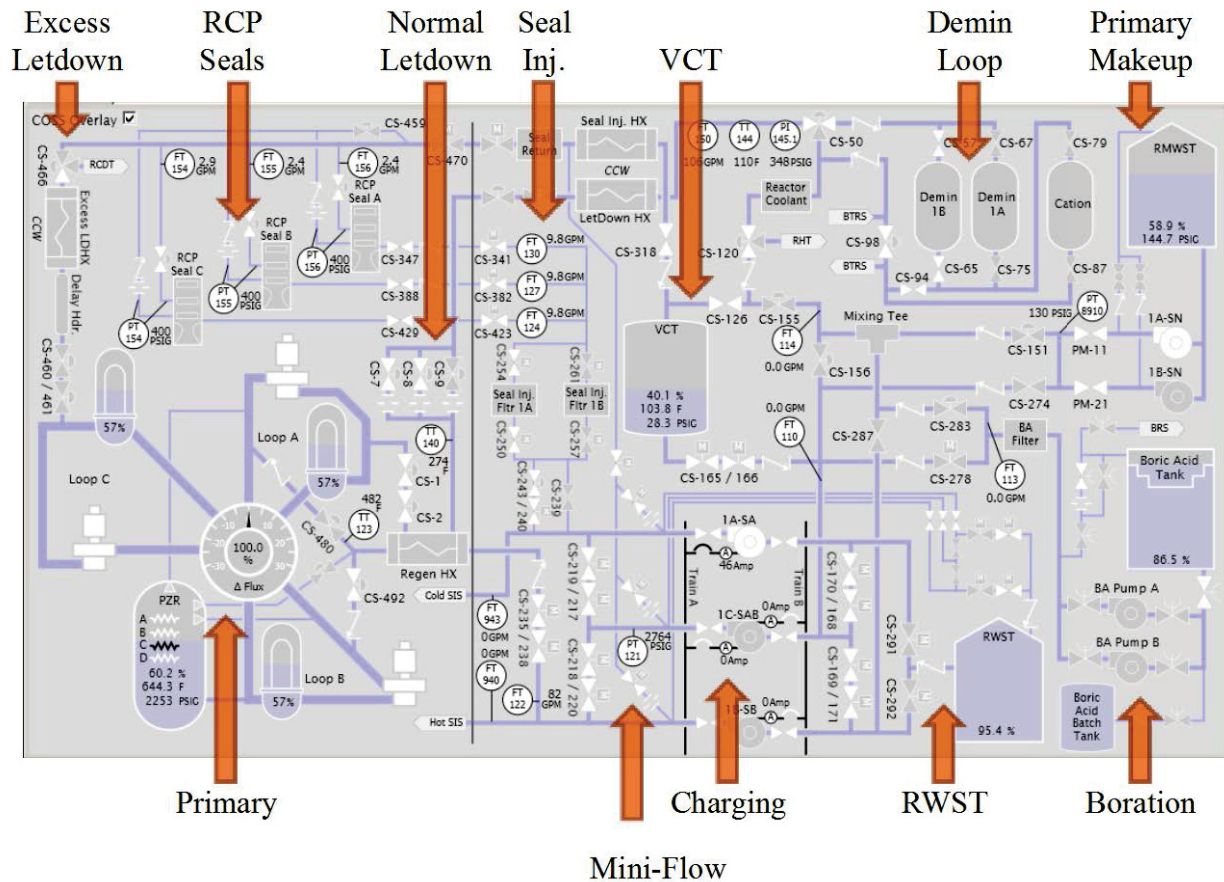


Figure 9 COSS P&ID main window depicting the CVCS and interconnected systems during a normal operating state.

The COSS uses a dullscreen display scheme comprised of grey, black, and white for denoting components in normal operating conditions and displaying computer-based procedures. Dullscreen denotes a display philosophy in which only items requiring operator attention have color, while all remaining items are presented in black, white, or greys. Thus, yellow and red are used judiciously to denote warning and alarm states, respectively. The color blue is used to depict potential sensor failures in the trend alarm panels. The color green is used exclusively by the recommender system, both for messages to the operator and for highlighting areas of concern in the P&ID display. Descriptions and explanations of the individual display components will be provided in the sections below.

#### 4.3.2 Status Indicator and Menu

The COSS operates continually to monitor system status. The status indicator informs the operator that the COSS is functioning properly at any given point in time. The status indicator is located in the top left corner of the COSS display (see Figure 10). The status indicator consists of a green circle and COSS label highlighting that appears and disappears in a continuous cycle. In the event that the COSS malfunctions, the frozen state of the green circle and COSS label provide immediate feedback that the system has stopped functioning properly.



Figure 10 COSS status indicator and navigation buttons.

Adjacent to the COSS status indicator is the menu of available views to display in the main window area (see Figure 10). The COSS can toggle between three views: P&IDs, Procedures, and Trends. The currently selected item is highlighted with a white border for easy identification. P&IDs is the default view. Procedures will display the currently active procedure, with additional procedures denoted as separate tabs. The Trends button invokes a detailed view of one of the trend alarms normally found on the right of the screen.

### 4.3.3 COSS Recommender System

The recommender system is located along the top of the COSS interface, adjacent to the menu. The recommender system provides a visual presentation of the detection, validation, diagnosis, and monitoring functions completed by the COSS. When the COSS detects a fault, a warning display highlighted with a green background appears in the recommender area as can be seen in Figure 11. The warning display also contains a description of the trend that triggered the COSS to detect a fault, i.e. “Detected unintended loss of reactor coolant system (RCS) inventory.”

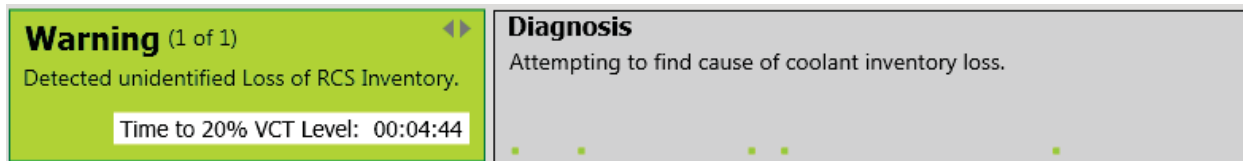
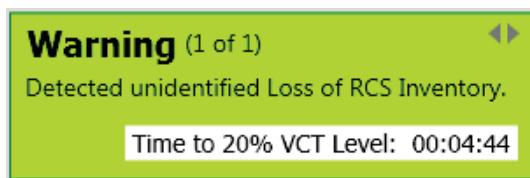


Figure 11 Recommender system presenting a warning with the shot clock and diagnosing the fault.

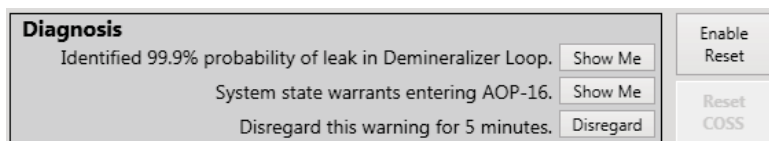
In the current prototype, the COSS mimics but does not perform actual sensor validation and fault diagnosis in real time. The validation and diagnosis functions mimicked by the COSS require time to assess trends and validate sensor values. Due to the time requirement, the recommender cannot provide instantaneous suggested mitigation actions. The recommender displays a progress bar to inform the operator that the COSS is currently in a validation or diagnostic state. The progress bar can be seen along the bottom of the message section of the recommender system (see Figure 11). Providing this information is important to convey that any information currently presented may change based on the outcome of the validation and diagnosis processes. If the COSS system enters this state, the operator should wait until the COSS finishes these functions to ensure that the recommender presents the most appropriate and current faults and mitigation actions.

The COSS has a predictive capability that allows it to determine future trends for each component. Analyzing future trend states allows the COSS to provide the operator with a *shot clock*. The shot clock provides the operator with the predicted amount of time before the fault reaches a safety critical set point that requires a reactor trip or other safety actuation (see Figure 12). A tooltip help message reminds the operator of the outcome should the shot clock reach 00:00. Providing the predicted amount of time before an alarm allows the operator to prioritize diagnostic and mitigation activities. With ample time, the operator can conduct more diagnostic and mitigation activities. In contrast, when there is little time to act the operator can take a more drastic mitigation activity that requires less time.



**Figure 12** Shot clock tooltip.

After the validation and diagnosis processes are complete, the message section of the recommender system provides a description of the cause of the fault, recommended action descriptions, and “Show Me” buttons that allow the operator to select particular mitigation actions. Selecting “System state warrants entering AOP-016” (see Figure 13) automatically displays the appropriate operating procedure. The operator can navigate back to the P&ID from the CBP from the recommender system or the COSS navigation menu buttons. Selecting “Identified 99.9% probability of leak in Demineralizer Loop” will display the P&ID with relevant areas of concern highlighted in green.



**Figure 13** Recommender message section containing "Show Me" buttons that link to the P&ID and procedure and the disregard button. Also present is the "Enable Reset" and "Reset COSS" buttons.

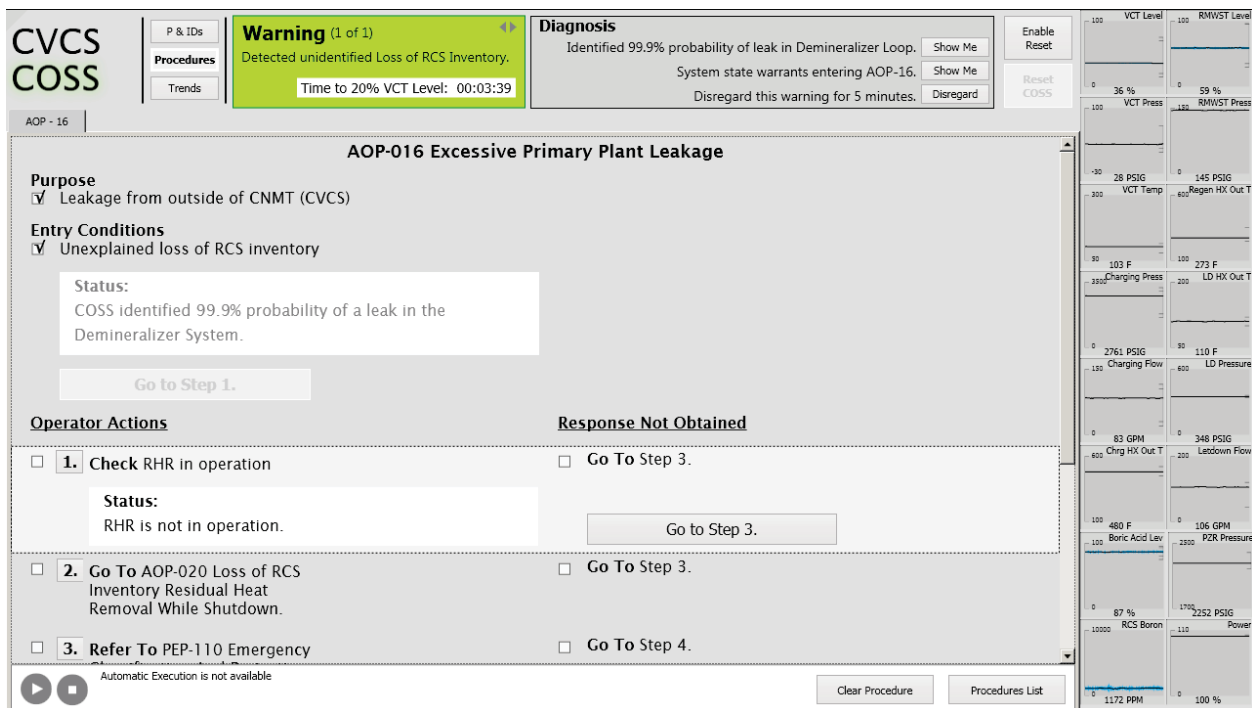
Though the recommender provides suggested mitigation actions, the operator ultimately determines whether or not to initiate those actions. In the event the operator has reason to disagree with the suggested mitigation action, the disregard button can be selected to turn off the COSS warning. The operator can then navigate to the CBP view and select the “Procedures List” button to display a list of procedures for manual selection.

The operator can activate the “Reset COSS” button by selecting the “Enable Reset” and then selecting “Reset COSS” to reset the COSS warning (see right side of Figure 13). After selecting reset, the COSS may detect the same trend as before, which triggers another fault and displays the same warning, diagnosed cause, and mitigation actions. The reset function enables the operator to trouble shoot potential COSS malfunctions.



#### **4.3.4 Computer-Based Procedures**

CBPs are central to the COSS since they support the primary interaction method between the operator and the system. The CBPs begin with the purpose and entry conditions as determined from the fault diagnosis. The CBPs resemble traditional paper procedures used throughout nuclear power plant operations (see Figure 14). The procedures are displayed in a two-column format. The left column contains the Operator Action steps, and the right column contains the Response Not Obtained steps. Each step in both of the columns contains a box with the information required to complete the action, buttons to navigate to the correct step, and a check box that is automatically checked off when the operator completes the step by selecting the appropriate button. The Response Not Obtained has procedure navigation buttons that allow the operator to move to the appropriate step when the desired response was not obtained. A light grey box highlights the current step, and the information boxes and buttons become active as indicated by black borders and text. Previously completed information boxes and buttons are grey to indicate they are no longer updated by the COSS or capable of manipulation by the operator.

Often, procedures require entering additional procedures before moving to another step within the current procedure. The COSS supports entering multiple procedures with buttons embedded within the procedure steps that allow the operator to open the additional procedure in another tab and display that procedure. After completing the necessary steps for this additional procedure, another button embedded within the additional procedure allows the operator to return to the original procedure. The operator can also use the tabs to navigate between procedures outside of the guided method with the embedded linking buttons to additional procedures. Within procedures the operators also must have the flexibility to return to previous steps if the need arises. The number for each step serves as a button that allows the operator to return to that step at will. Returning to a previous step clears any previous selections for any steps following the selected previous step. Additionally, the values and states for the status messages are cleared and updated by the COSS once the operator reaches the step again. Detailed specifications for CBPs depicted in the COSS prototype can be found in Appendix A.



**Figure 14 Computer-based procedure depicting the active step with a light grey background, a step status message, and a "Go to step" button in the active state.**

The current CBP prototype allows both Step-by-Step execution and Automatic Execution of sequences of multiple steps. The run and stop buttons (denoted by  and , respectively) are used to toggle automatic execution and can be seen along the bottom of Figure 14. When Automatic Execution is possible, a text description of the sequence of steps message appears next to the run and stop buttons. Additionally, black is used to denote a selectable state for the run and stop buttons. For example, if the Automatic Execution is in effect, the stop button is highlighted in black to indicate it can be selected, and the run button is grey to indicate that it cannot be selected.

#### 4.3.5 Piping and Instrumentation Diagrams





immediate access to trend and current indicator values for components. Additionally, all warnings and alarms are immediately visible while the operator is completing the computer-based procedures or interacting with the P&ID. The 16 trend alarms selected for the COSS interface provide information for CVCS relevant components and subsystems, such as the volume control tank, charging pumps, letdown flow, and the boration and dilution system. The trend alarms serve as salient warning and alarm indicators in situations in which a component's sensor reaches a predetermined set point.

Each trend alarm contains a trend line, warning and alarm anchor bars, and the current component value. During normal plant states the trend lines are fairly stable and flat. Deviations away from a straight line across the alarm contrasts the rest of the trend line alarms within the panel to alert the operator of a fault. Due to normal plant adjustments, predicted trend deviations do not necessarily indicate an abnormal state. The trend alarms use background color to denote any trend that crossed into a warning or alarm state. The trend alarms are grey while the current value of the trend is within normal operating parameters. When a trend reaches a particular set point, the trend alarm panel background turns yellow to alert the operator that the trend has reached a warning state (see "LD Pressure" indicator in Figure 16). The trend alarm background changes to red when the trend reaches an alarm state (see "VCT Level" and "Boric Acid Lev" in Figure 16). The trend alarms also contain warning and alarm bars that provide the operator with contextual information depicting the warning and alarm ranges for a particular trend alarm. At all times, the current component value is displayed at the bottom of the trend alarms.

The trend lines represent a component's state based on values from multiple sensors physically located on the component. The trend alarm panels support the operator in sensor failure detection. The COSS monitors the sensors and displays confidence intervals around the trend line to provide the operator with real time estimates concerning the accuracy of the trend line. The confidence interval is displayed as a blue area around the trend line. As the sensor value drifts away from other sensors on a component, the confidence interval expands (see "Boric Acid Lev" in Figure 16). The blue highlighting serves as a salient indicator when faulty sensor values are detected by the COSS. When the sensors are in alignment with each other, the blue confidence interval is not visible.

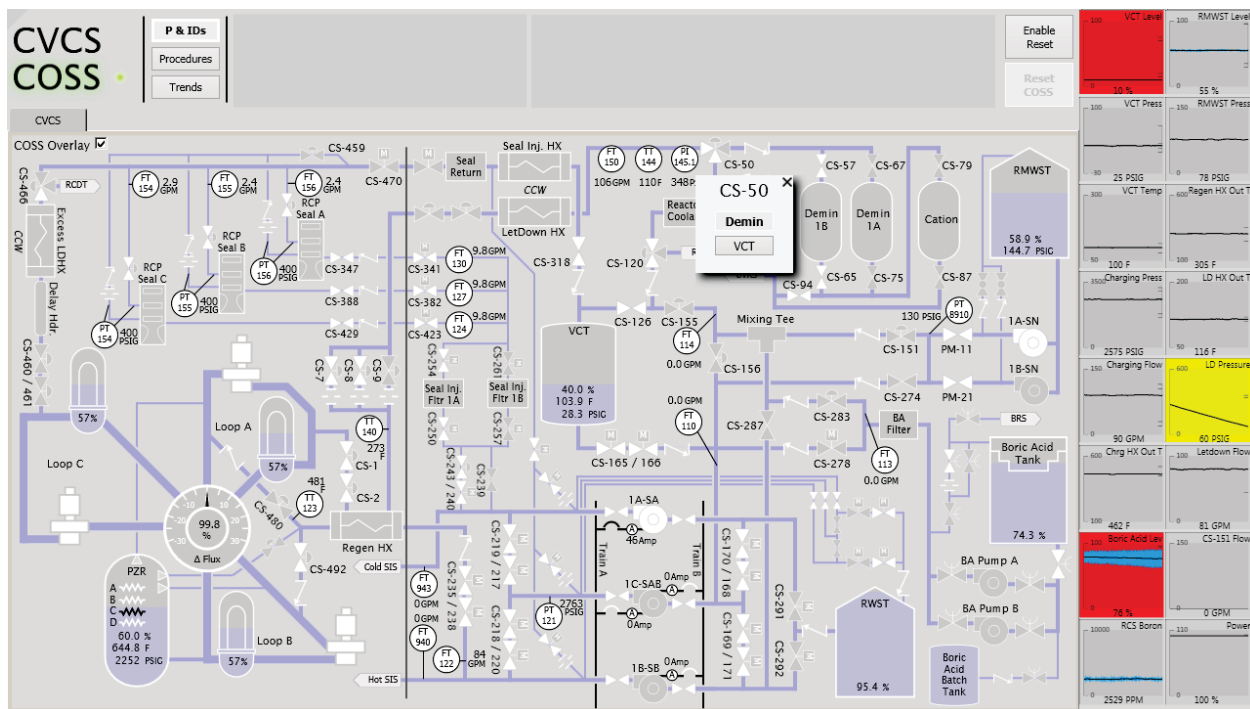


Figure 16 COSS display featuring trend alarms that have reached warning, alarm, and sensor drift and failure states.

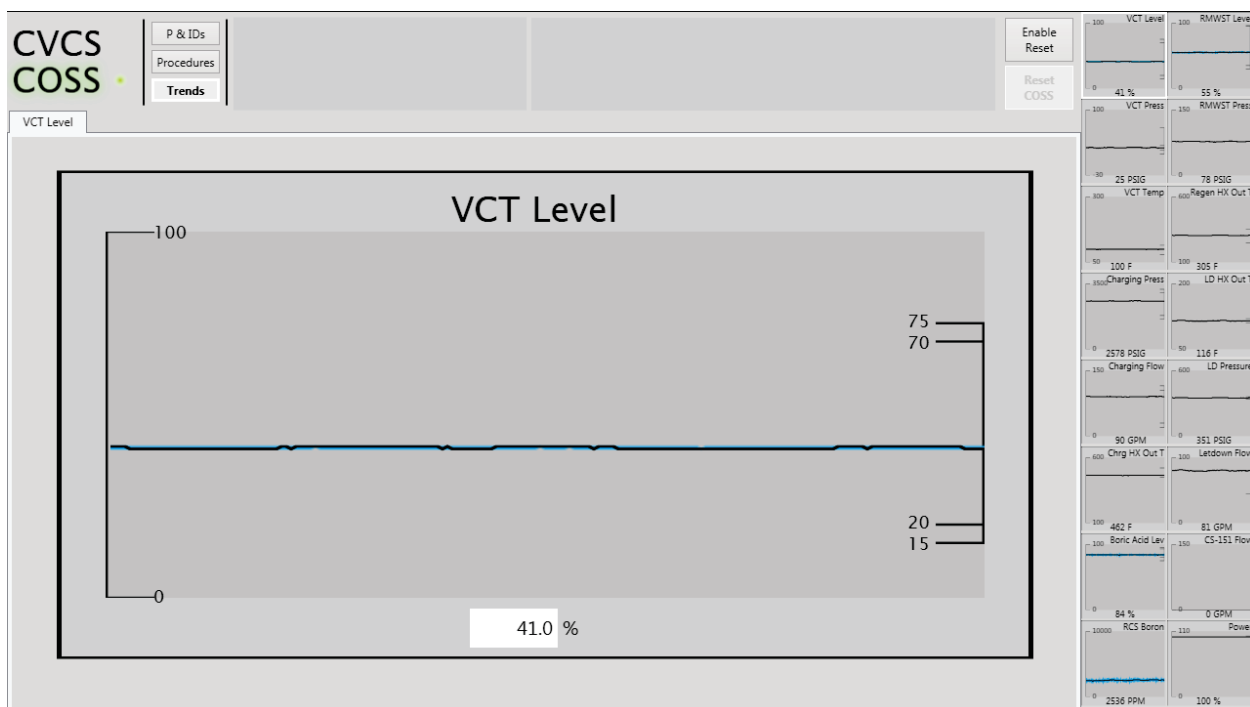


Figure 17 Expanded trend view from one of the trend alarms.

Clicking on one of the trend alarm displays brings up an expanded view of that trend in the main display area (see Figure 15). The corresponding “Trends” navigation menu button is highlighted, as is the mini

trend alarm display box on the right of the display. The expanded view allows the operator to track in greater detail and with easier legibility the state of a particular plant indicator. Such trending is especially important during plant transients and during recovery actions to restore plant functions.

### 4.3.7 Navigation

There are several ways to navigate throughout the different COSS screens. Three buttons located next to the COSS status display allow the operator to switch between the computer-based procedures, the P&ID, and detailed trend alarm views (see Figure 18). When in the Procedures view, the operator can move between opened procedures by selecting the tab containing the desired procedure number (see Figure 18). This tab is located directly above the currently opened CBP. Operators can manually access other procedures by selecting the button labeled “Procedure List” located in the bottom right portion of the CBP view. The same tab and list navigation scheme is used to move between different P&ID sections. In addition to tab navigation, selecting link buttons embedded within the P&ID allow the operator an alternative method to access related systems. When in the P&ID view, selecting a particular component opens a pop-up menu containing more detailed information and controls for that component. Selecting the close button on the pop-up menu removes the window so that all components in the current P&ID are visible. Finally, the recommender system provides buttons that take the operator to the desired mitigation action related procedure or the P&ID with highlighted faults.

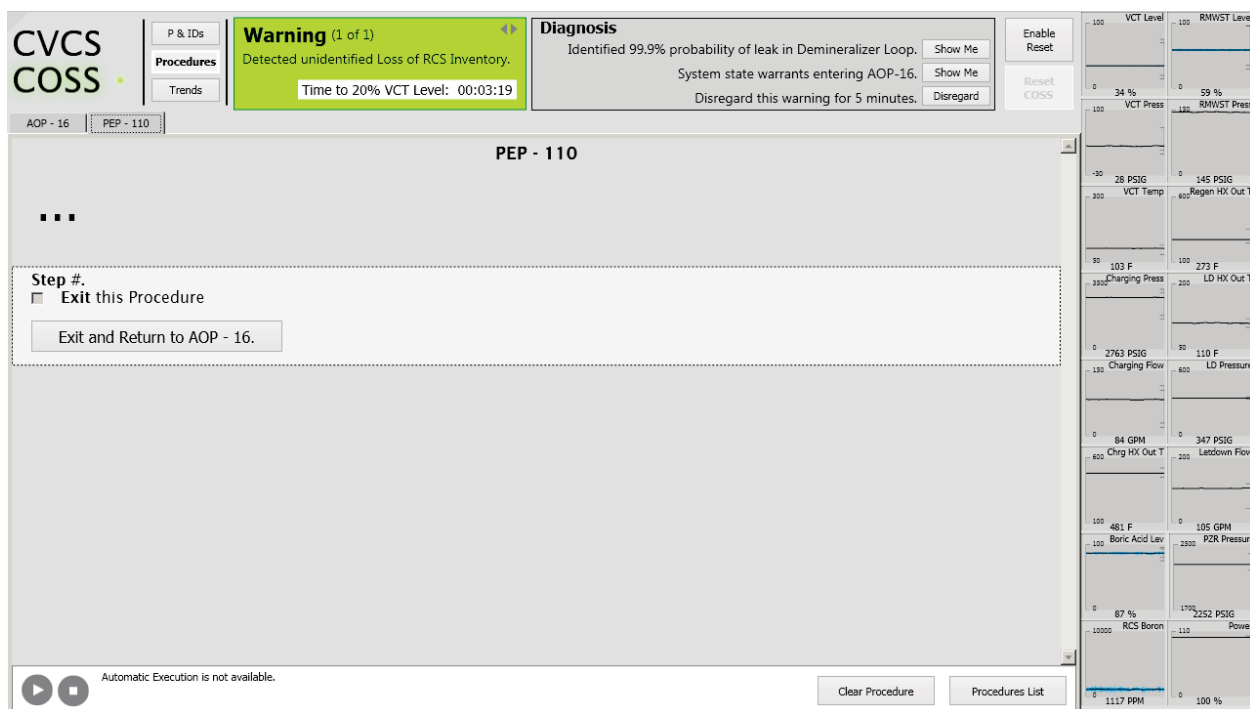


Figure 18 COSS display depicting multiple selectable tabs for different computer-based procedures.

## 4.4 Leaking Demineralizer Scenario Walkthrough

### 4.4.1 Fault Detection

The scenario initiates with the plant in steady state operating conditions. The trend alarm panels are all



The VCT level trend alarm shows the decreasing trend for the VCT level, but the COSS detects the trend before the alarm reaches its warning set point. Due to the early detection, the mitigation actions may be completed before a warning set point is ever reached. Under the current procedure, the operator is required to determine whether the leak size is greater than VCT make-up capacity, and if so, manually trip the reactor. This is a conservative action to ensure that a low VCT level does not result in damage to the CVCS pumps. It is judged that the operator would have difficulty in diagnosing the location of the leak and whether it could be isolated in the time available, in contrast to the ability of the COSS to make this determination before a manual trip of the reactor is required.



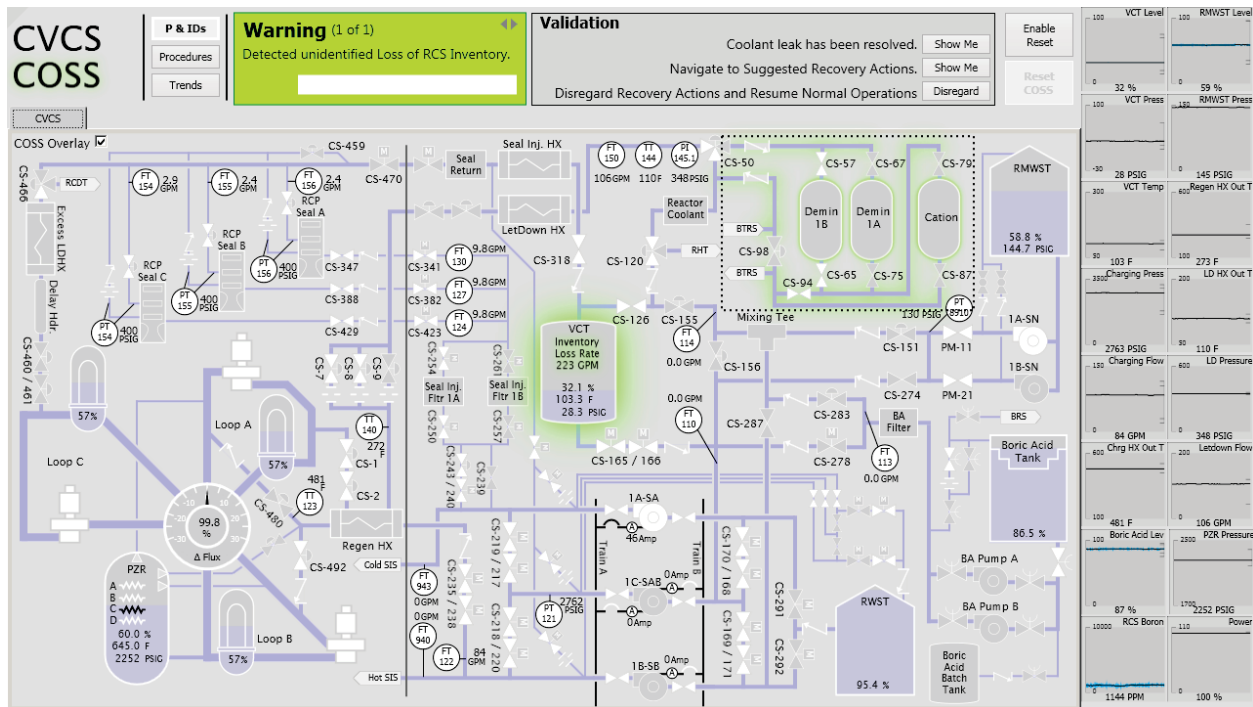


Figure 20 COSS display featuring the recommender identifying the leak and suggesting mitigation actions.

#### 4.4.2 Fault Validation and Diagnosis

During the fault validation and diagnosis, the recommender displays “Attempting to determine the cause of loss of reactor coolant inventory” along with a status bar (see Figure 19). These items are displayed in the message section of the recommender system. Once the COSS has validated and diagnosed that the fault is located within the demineralizer loop of the CVCS, the recommender system displays “Identified 99.9% probability of leak in Demineralizer Loop.” Note that this prototype only mimics PRODIAG fault validation and diagnosis in the current version.

#### 4.4.3 Fault Mitigation

After the COSS has validated and diagnosed the fault, the COSS recommender system displays a more detailed description of the fault directly on the P&ID. In this scenario, “Inventory Loss Rate 223 GPM” can be seen displayed on the VCT (see Figure 20). The COSS highlights the faulted section on the main P&ID in green to provide contextual information concerning functionally related components affected by the fault and the mitigation actions. In this case, the mitigation action is to align letdown around the demineralizers to isolate the leaking demineralizer system. The recommender system displays the message “System state warrants entering AOP-016.” AOP-016 is the abnormal operating procedure for excessive primary plant leakage and is based on the original procedures developed by Westinghouse. This particular scenario contains only one mitigation action, but in other scenarios there may be multiple mitigation pathways. In situations with multiple mitigation pathways, the preferred pathway that most ensures plant safety would be displayed top most, and each subsequent pathway would be displayed below in a list in priority order.

The operator can accept the suggested mitigation to display AOP-016 by selecting the button labeled “Show Me” next to the suggested mitigation message. The COSS displays the first page of the operating

procedures (see Figure 21). The operator can view the purpose and entry conditions for AOP-016. The diagnosis mandating entry into AOP-016 is also displayed in a white box near the entry conditions to serve as a reference in case another warning occurs and the diagnosis displayed by the recommender no longer pertains to the CBP currently being viewed. The operator acknowledges the purpose and entry conditions by selecting the “Go to Step 1.” button. Selecting the “Go to Step 1.” button checks the boxes next to the purpose and entry conditions statements to serve as both a log and a place keeping technique.

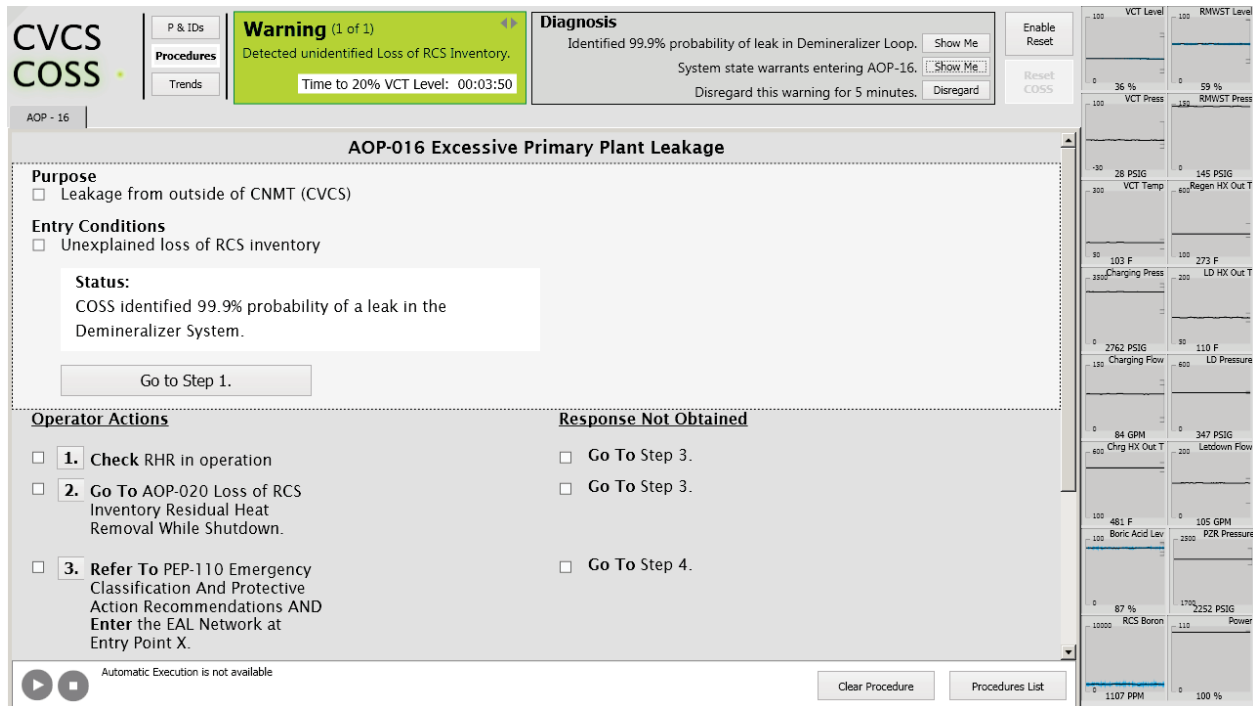


Figure 21 CBP displaying the purpose and entry conditions for AOP-016.

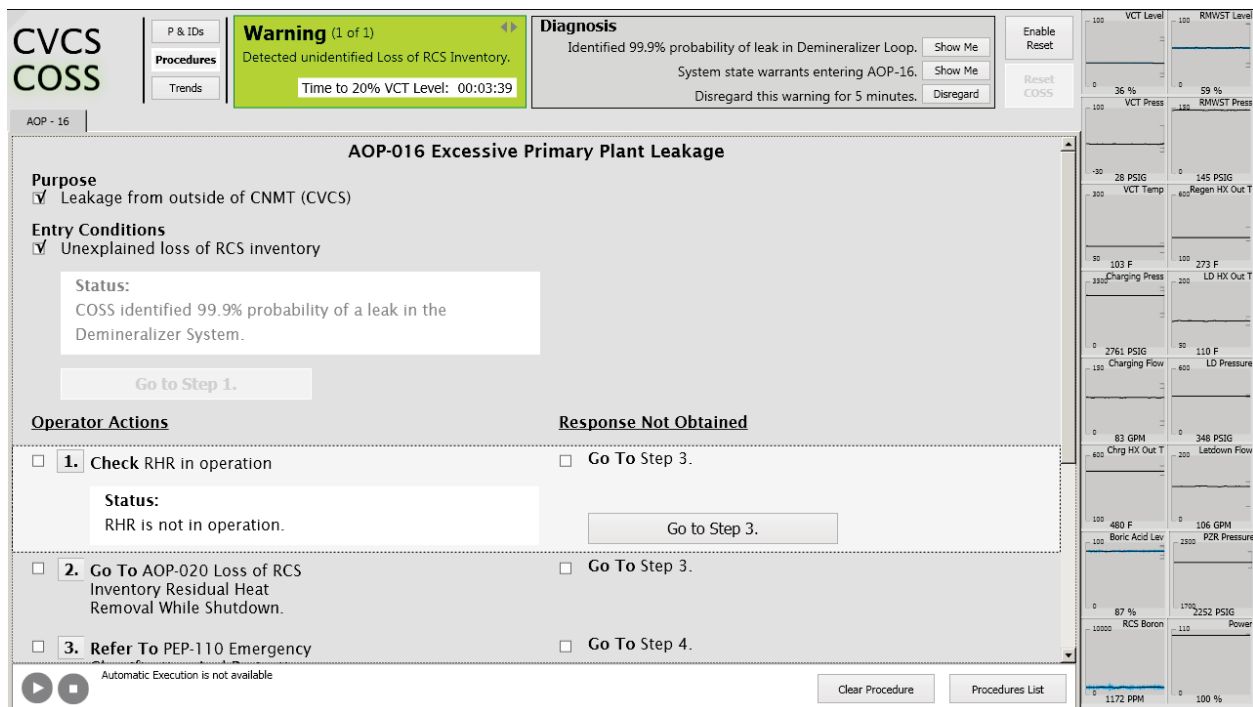
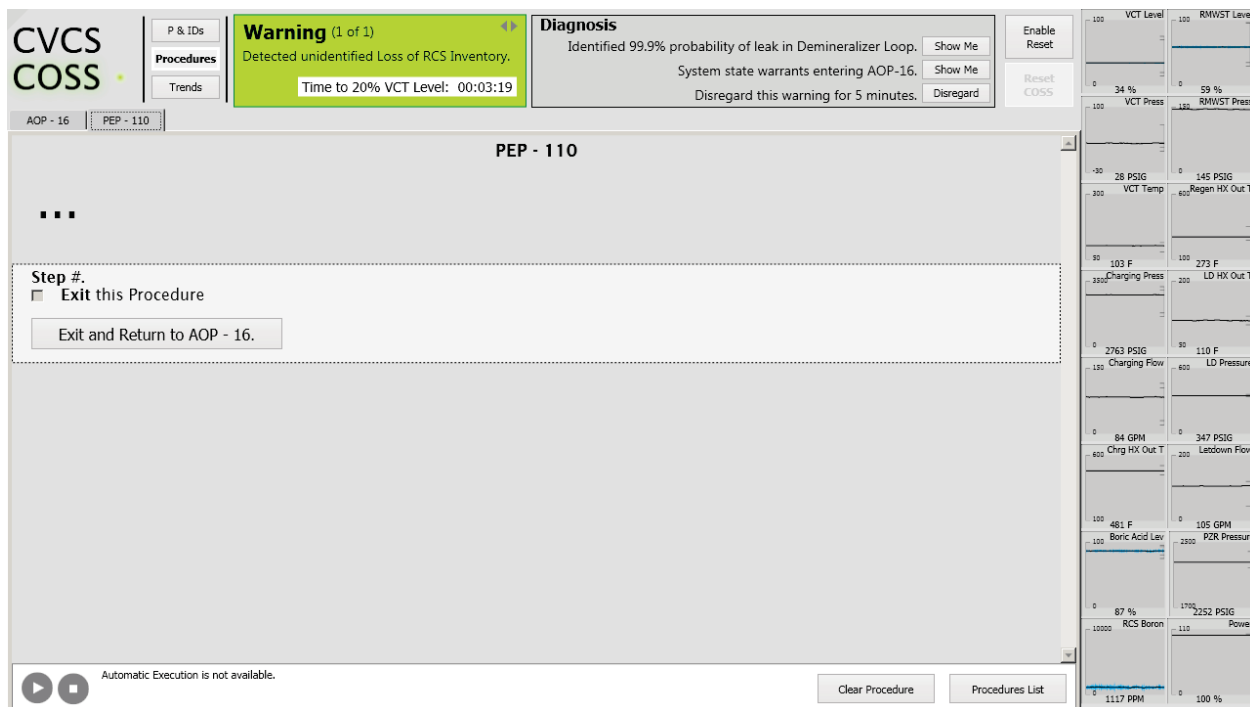


Figure 22 Computer-based procedure displaying the first step of AOP-016.

In this scenario residual heat removal (RHR) is not in operation as indicated by the information box located directly below the step. The operator then selects the “Go to Step 3” button, which automatically checks the box next to the response not obtained step and advances the procedure to the next applicable step (see Figure 22). In this scenario, step three is the next applicable step. As can be seen in Figure 23, step two was not completed. Italic font is used to denote that step two was not completed. The check boxes next to the operator actions and response not obtain text for step two remain unchecked as an additional indication the step was not completed. The active step three in Figure 23 depicts a step that requires the operator to enter procedure PEP-110.

The screenshot displays the CVCS COSS interface. At the top, a 'Warning (1 of 1)' box indicates 'Detected unidentified Loss of RCS Inventory' with a 'Time to 20% VCT Level: 00:03:29'. A 'Diagnosis' box shows 'Identified 99.9% probability of leak in Demineralizer Loop.' and 'System state warrants entering AOP-16.' Below these, a 'Go to Step 1.' button is visible. The main procedure area is divided into 'Operator Actions' and 'Response Not Obtained' sections. Under 'Operator Actions', step 1 is 'Check RHR in operation' with a status box stating 'RHR is not in operation.' Step 2 is 'Go To AOP-020 Loss of RCS Inventory Residual Heat Removal While Shutdown', which is italicized and has an unchecked checkbox. Step 3 is 'Refer To PEP-110 Emergency Classification And Protective Action Recommendations AND Enter the EAL Network at Entry Point X.', which is the active step with an unchecked checkbox and a button labeled 'Enter PEP - 110.' Step 4 is 'Isolate Demineralizer Subsystem' with an unchecked checkbox, and sub-step 'a. Align CS-50 to VCT' is also unchecked. The 'Response Not Obtained' section has checkboxes for 'Go To Step 3.', 'Go To Step 4.', and 'Go To Step 5.', with 'Go To Step 3.' being the active selection. A 'Go to Step 3.' button is also present. At the bottom, there are buttons for 'Clear Procedure' and 'Procedures List', and a note 'Automatic Execution is not available'. On the right side, there is a vertical strip of process parameter monitors including VCT Level, RMVST Level, VCT Press, RMVST Press, VCT Temp, Regen HX Out T, Charging Press, LD HX Out T, Charging Flow, LD Pressure, Chrg HX Out T, LD Flow, Boric Acid Lev, PZR Pressure, RCS Boron, and Power.

**Figure 23 Computer-based procedure depicting a step that requires the operator to enter another operating procedure before continuing the current procedure.**



**Figure 24 Computer-based procedure depicting procedure tabs and an exit procedure button.**

Completing PEP-110 (Plant Emergency Plan - 110) is outside the scope of the demonstration for this prototype. Future versions of the COSS incorporating additional functionality may include PEP-110, but to demonstrate the capabilities of the COSS for isolating a leak it isn't necessary to establish the overall plant emergency status. Only the last step of PEP-110 is depicted in Figure 24 to demonstrate how the operator exits the procedure and returns to AOP-016. After exiting PEP-110, the operator is returned to step four of AOP-016. Step four contains the mitigation actions for the demineralizer loop isolation by sub steps Align ICS-50 to VCT and Close ICS-98 (see Figure 25). The operator can manually select the button to align CS-50 to VCT. While the valve is diverting, a progress bar consisting of green circles moving clockwise in a circular fashion indicates that the selected action is in process. While the valve is diverting, the text on the "Align CS-50 to VCT" button changes to "Abort Aligning CS-50 to VCT" to allow the operator the ability to abort the action taken for this step. The operator would then be able to manually complete the action again if desired and then select the next step, "Close CS-98" to complete the demineralizer loop isolation. At any time, the operator can select the run button located along the bottom of the display to automatically execute the remaining steps of a sequence (see Figure 25).



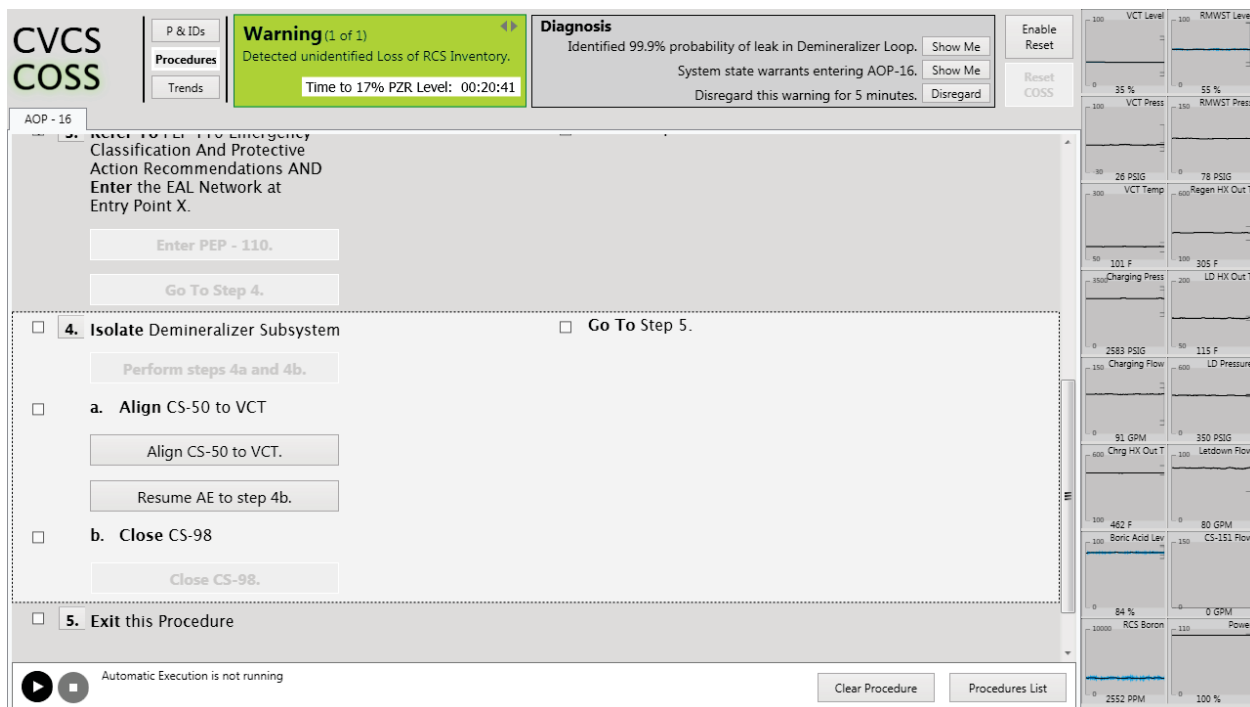


Figure 26 Computer-based procedure depicting the selection of the "Resume AE to step 4b." button and the feedback indicating automatic execution is enacted.

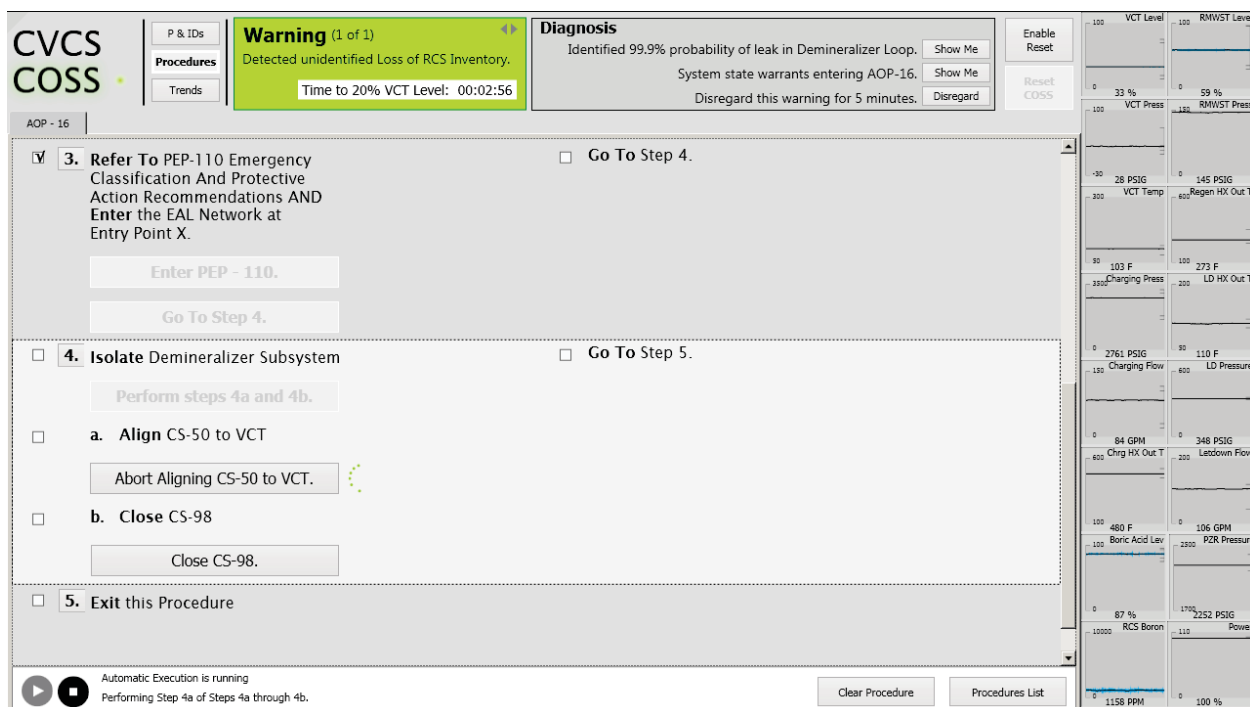


Figure 27 Computer-based procedures depicting the "Automatic execution of steps 4a through 4b." initiated by selecting the run button located along the bottom of the display.



## 4.4.4 Fault Monitoring and Validation

Once the operator has completed all the CBPs for the mitigation actions, the COSS system continues to monitor the CVCS to determine that the actions were successful. During this monitoring phase, an enlarged trend alarm display for the VCT level can be displayed in the main window area to provide more detailed trend information. After the COSS determines that the VCT level trend has reached a stable point and is no longer decreasing, the recommender provides a message that the system is stable. If no other warnings or recommendations are present, the recommender warning and message sections are removed to leave a dull greyed area that reduces display clutter.

## 4.4.5 Resume Normal Operations Suggestions

The COSS has aided the operator in successfully avoiding a plant trip by mitigating the leaking demineralizer fault. The COSS provides the operator with suggestions to resume normal operations (see Figure 28). The VCT level has been stabilized, but it is lower than the desired operating range. In this particular scenario, selecting “Navigate to Suggested Recovery Actions” would display “Enter OP-107.03 CVCS Fill, Vent, and Maintenance Activities to restore the VCT level to within normal operating ranges.” The operator can also select the “Disregard” button if he or she wishes to manually open and complete a different set of procedures.

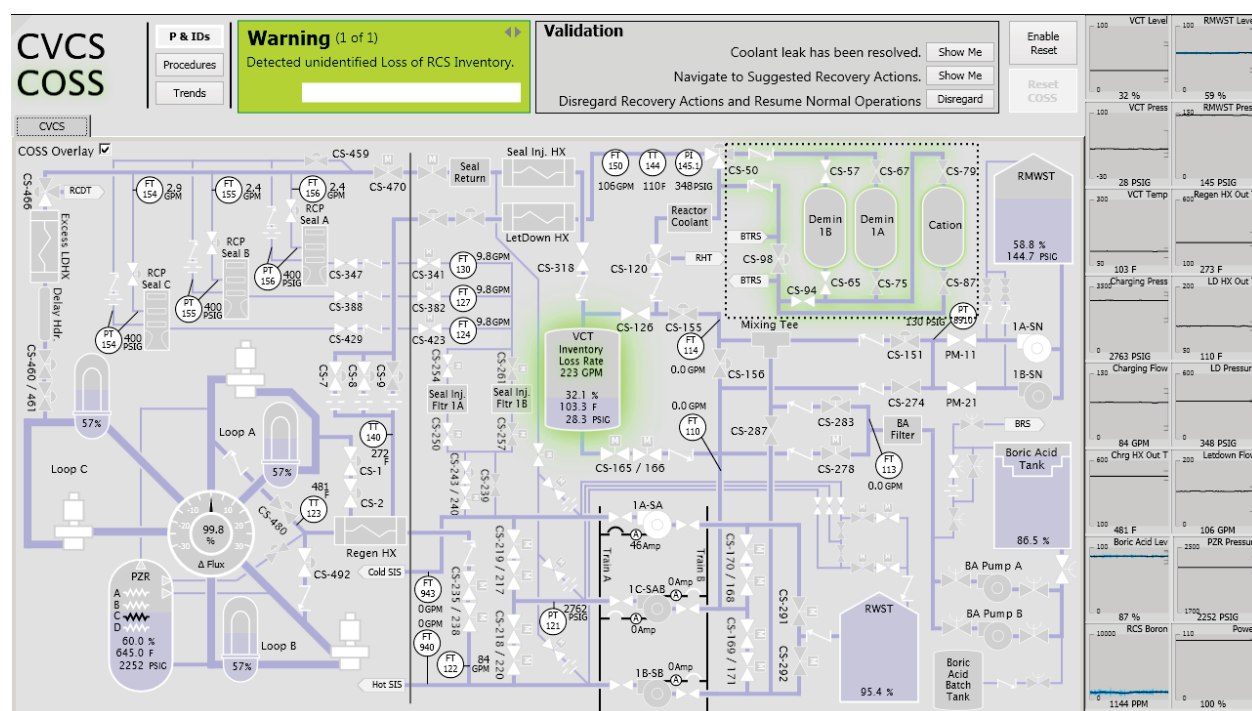


Figure 28 COSS display featuring the validated resolution of the coolant leak and the option to navigate to suggested recovery actions.

## 4.5 CSIP Trip Scenario Walkthrough

### 4.5.1 Fault Detection

The scenario initiates with the plant in steady state operating conditions. The trend alarm panels are all within normal operating ranges, and the COSS status indicator is pulsing to convey that the system is



functioning properly. Then, a fault is triggered to simulate a Charging and Safety Injection Pump (CSIP) trip. Upon activation of the fault the COSS immediately registers the trip on CSIP A (see Figure 29). The COSS warning area background changes to green and displays the text “CSIP A Trip or Close Circuit Trouble”. The corresponding CSIP A pump indicator is highlighted on the P&ID. A shot clock is also displayed in the warning area to provide the operator with the amount of time before the pressurizer reaches the low level alarm setpoint of 17% capacity. The recommender area displays the text “Attempting to find cause of CSIP A Trip”. The trend alarm for the charging flow and seal injection flows trend alarms transition from grey to yellow and to red within seconds as the charging flow and seal injection flow trend indicators decrease to zero in response to the CSIP trip. The absence of the charging flow results in a rise in the regenerative heat exchanger temperature. The pressurizer level continues to decrease around two percent per minute.

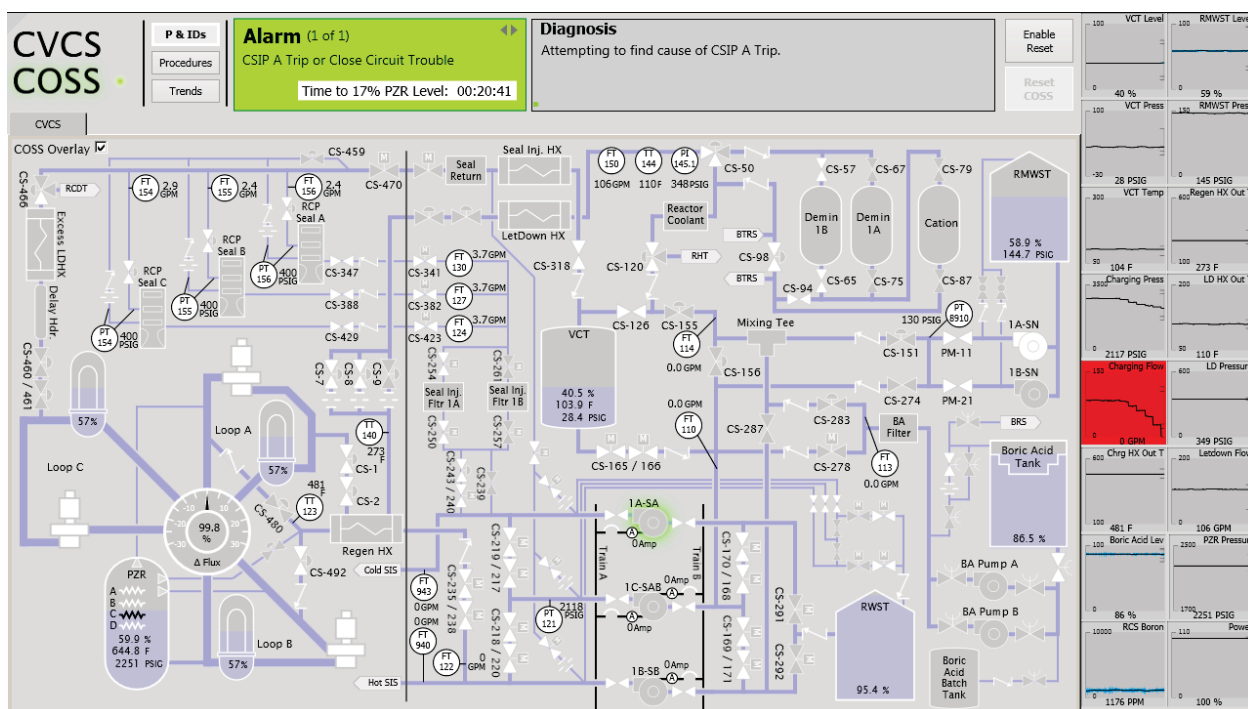


Figure 29 COSS warning area stating the CSIP A Trip, recommender diagnosing status, and CSIP A highlight on the P&ID.

#### 4.5.2 Fault Validation and Diagnosis

During the fault validation and diagnosis, the recommender displays “Attempting to determine the cause of CSIP A Trip” along with a status bar (see Figure 29). These items are displayed in the message section of the recommender system. CSIPs can trip for a number of reasons including electrical and mechanical faults, however based on operational experience CSIPs are known to spuriously trip. When the COSS validates sensor data and fails to diagnose a direct cause for the CSIP A trip, the recommender system displays “Unable to identify cause of CSIP A Trip” with a “show me” button that allows the operator to navigate to the P&ID to acquire additional information and controls for CSIP A (see Figure 30). The recommender system also displays “System state warrants entering APP-ALB-06” with a “show me” button that allows the operator to navigate to the CBP for Annunciator Panel Procedure Alarm Light Board – 06 Unexplained CSIP Breaker Trip.

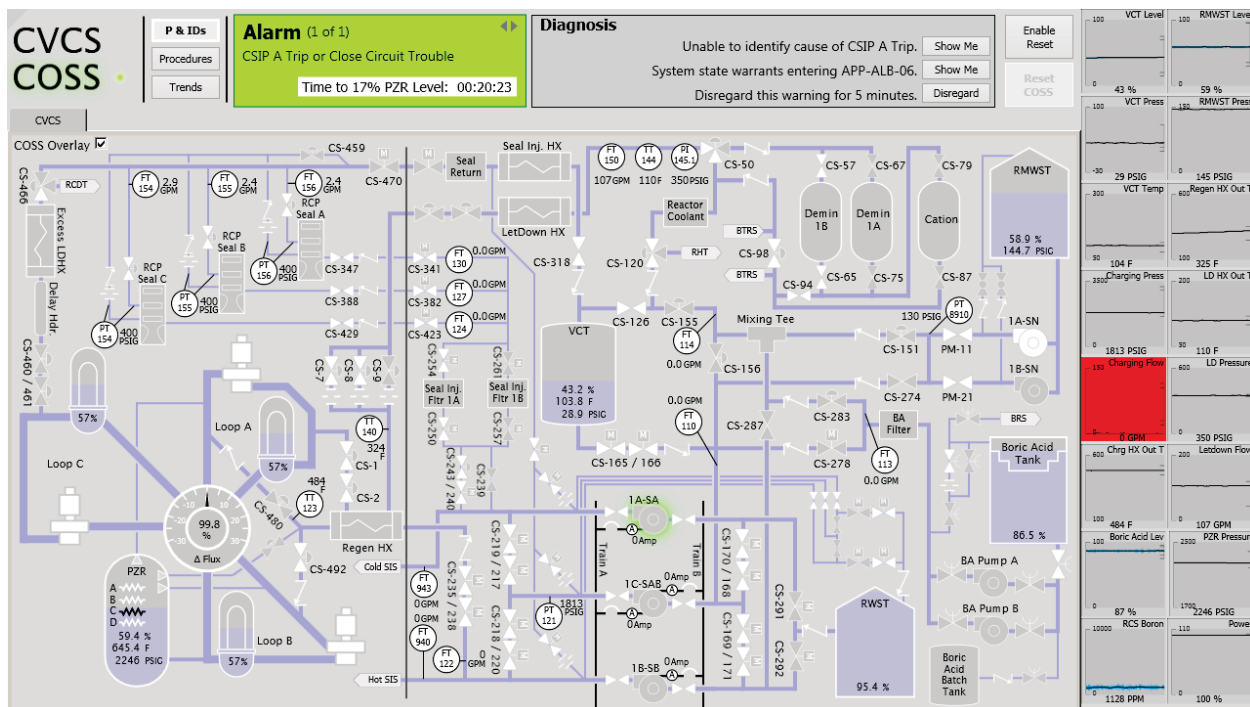


Figure 30 COSS recommender displaying the option to enter the APP-ALB-06 CBP because the cause of the pump trip could not be identified.

### 4.5.3 Fault Mitigation

The operator first attempts to restart CSIP A by selecting the “Restart CSIP A” button located within step one. CSIP A fails to restart suggesting CSIP A did not just spuriously trip (see Figure XX [need red X screenshot]). A green aura highlights CSIP B on the P&ID to direct the operator’s attention in conjunction with step 3 of the CBP. A highly salient red X is displayed on CSIP A after the failed restart to ensure the operator is aware CSIP A failed when in the P&ID view. Once the operator is done interacting with the COSS, selecting “Disregard” will close the COSS windows and remove the red X label from the P&ID (see Figure 31). A subtle cue to the CSIP A malfunction in the form a crack on the CSIP A symbol. The less salient cue reminds the operator that CSIP A is out of service, but should not interfere with normal scanning patterns across the P&ID. The operator is guided to the Response Not Obtained column of the CBP in which the operator places CSIP A in the manual off mode by selecting the “Stop CSIP A.” button. This ensures CSIP A does not automatically attempt to start until it has been properly serviced. At this point in the scenario, several of the trend alarms have reached warning and alarm states, which is readily accessible to the operator due to the persistent visibility of the trend alarms. The operator then proceeds to step two, which consists of starting CSIP B (see Figure 32). The COSS provides a green aura around CSIP B in the P&ID View. The operator selects the “Start CSIP B” button. Upon a successful CSIP start, the “Start CSIP B” button is no longer enabled and the “Go To Step 5.” button automatically becomes enabled to allow the operator to proceed to the next step, which exits the procedure.

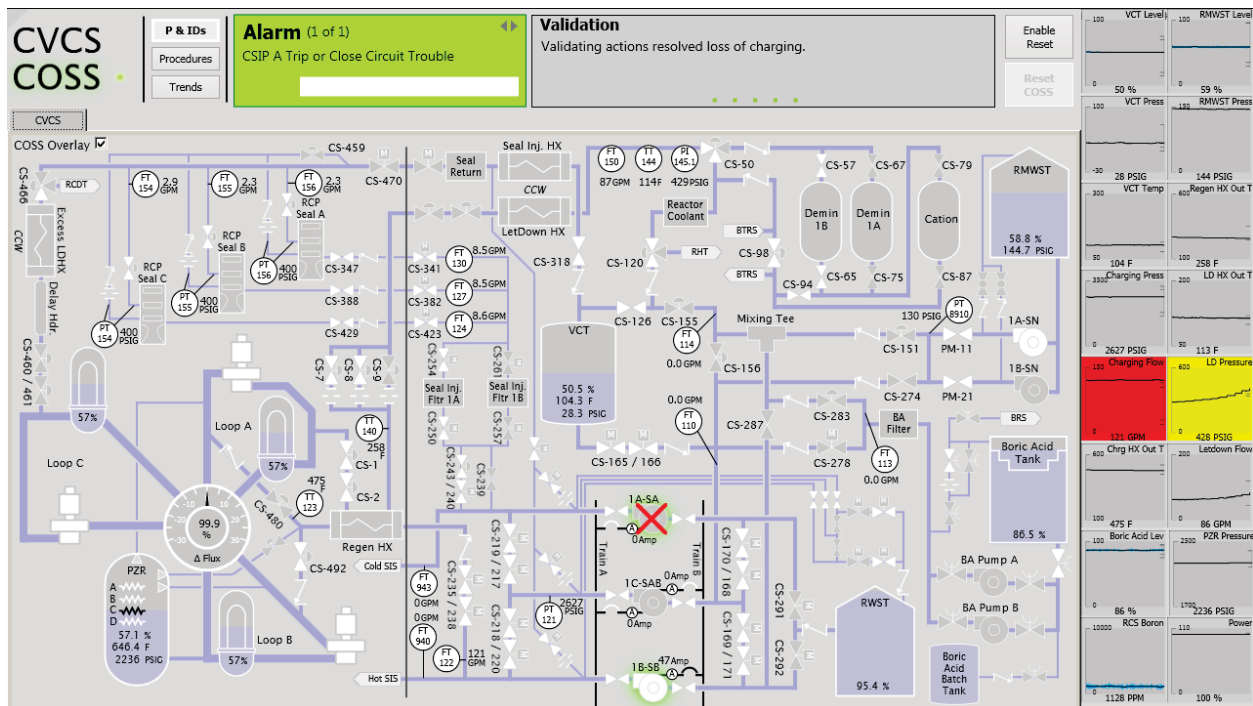


Figure 31 COSS depicting the validation of the mitigation actions taken to start CSIP B and restore charging flow.

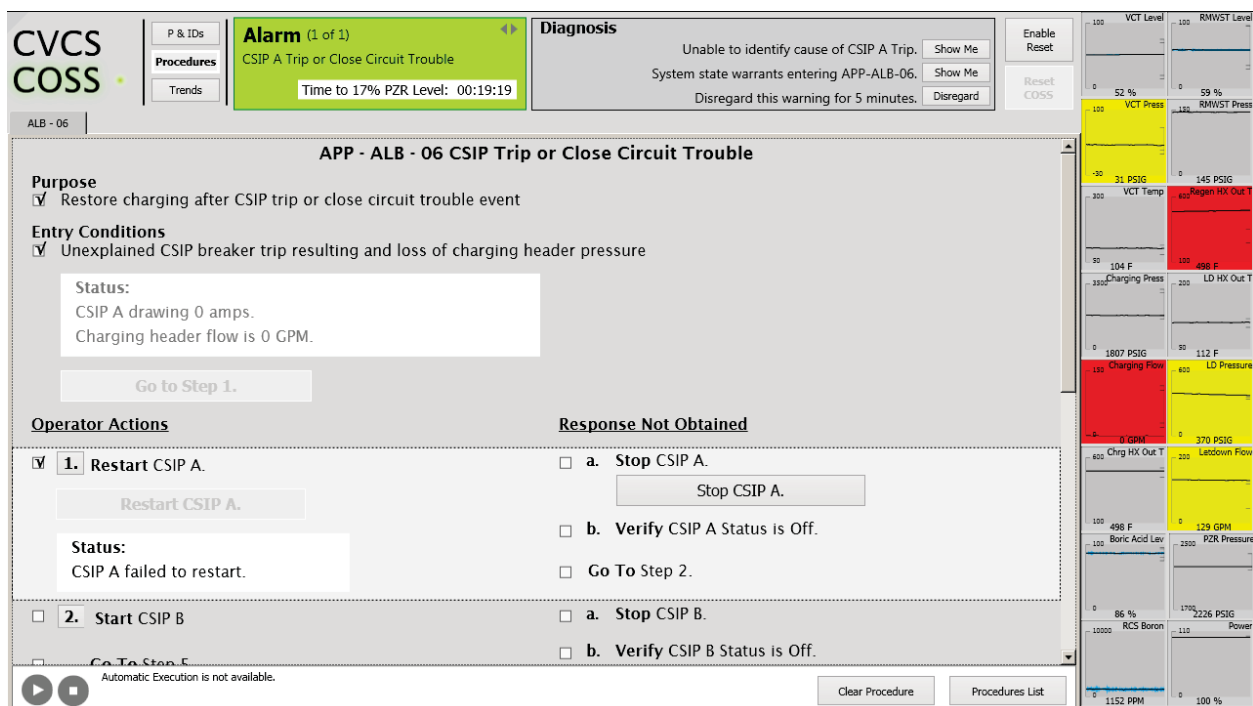


Figure 32 CBP view depicting the CSIP A failure to restart message in the information box and the automatic activation of the buttons in the response not obtained column.

## 4.5.4 Fault Monitoring and Validation

Once the operator has completed all the CBPs for the mitigation actions, the COSS system continues to monitor plant health. After the COSS determines that CSIP B is energized and charging flow and pressure have been reestablished, the recommender provides the message “Loss of charging has been resolved”. If no other warnings or recommendations are present, the recommender warning and message sections are removed to leave a dull greyed area that reduces display clutter (see Figure 33).

## 4.5.5 Resume Normal Operations Suggestions

Due to the complex dynamics resulting from the loss of charging flow some plant states may take some time to return to equilibrium. The operator can monitor the P&ID and trend displays to oversee the plant states are trending in the correct direction. For example, the regenerative heat exchanger will take some time to cool to its normal operating temperature.

Once the plant has reached a steady state the COSS prompts the operator with suggested recovery actions for the CSIP A trip event. In this particular scenario the suggested recovery action could entail alerting maintenance and completing a lock-out tag-out CBP to allow maintenance to safely service the pump. An example of a lock-out tag-out on the P&ID can be seen in Figure 33. The operator can click on the lock out tag out symbol to display a dialog containing detailed information about CSIP A (see Figure 34).

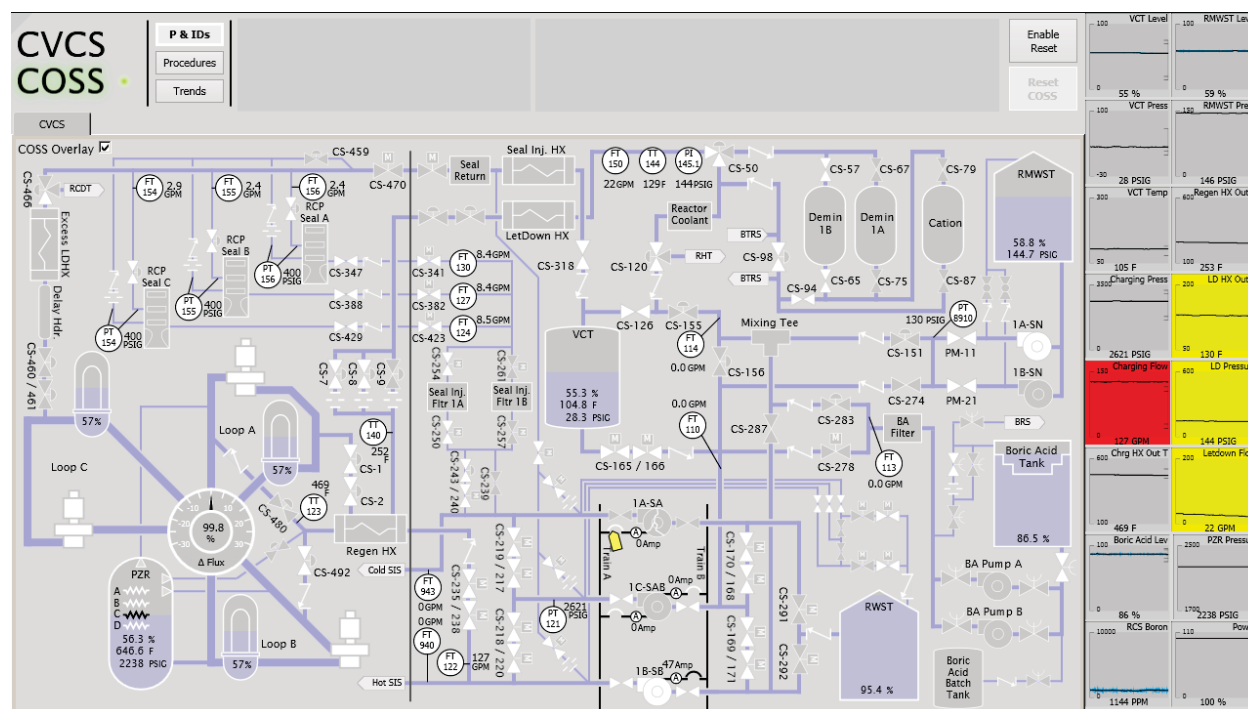
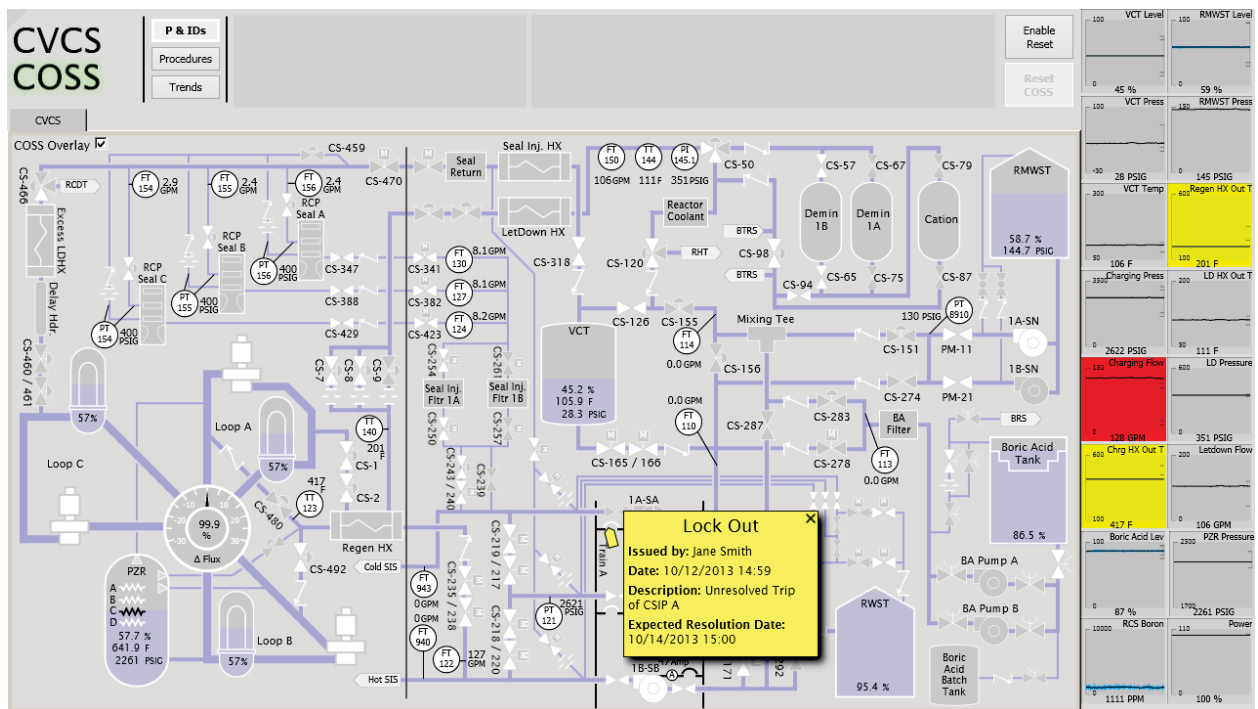


Figure 33 A lock out tag out symbol is overlaid on the breaker for CSIP A after the operator selects the “Disregard” button next to the recommender message “Disregard the warning for 5 minutes”.



## 5. Future Research

### 5.1 Real-Time Interface with Sensor Validation and Fault Diagnosis

Several areas of future research were identified in the development of the COSS prototype. The research will improve the underlying components of the prototype to expand its applicability to additional types of plant upsets. It will involve work in both the technology components as well as the human factors in the use of a COSS.

### 5.2 Enhanced Plant Instrumentation

The instrumentation that is currently installed in operating nuclear plants is that which is needed for plant protection and control purposes. Instrumentation is expensive to add, not only for the cost of the devices, but also the cost of installing instrument and power cables. It was designed to provide information to operators and systems on whether the plant was operating within acceptable boundaries and not for specific fault diagnoses. For example, the plant instrumentation might be able to confirm that there is a leak downstream of the instrument location, perhaps due to decreased pressure and increase flow, but not be able to tell specifically which component has the leak. Affordable, enhanced instrumentation would improve the accuracy of plant diagnoses and could perhaps be cost-justified by the reduction in plant upsets.

- *Enhanced Plant Instrumentation:* However, there are advancements in instrumentation now available or under development that hold promise for increasing the availability of a class of additional plant instrumentation to augment the COSS fault diagnostic function. These advancements include wireless signals, self-organizing instrument meshes for instrument networks, and power harvesting for instrument power from sources such as light, heat, vibration, etc. The instrumentation would not have to be safety-grade because it would not perform a safety-related function. A key consideration is the need to minimize the maintenance burden for additional instrumentation. So the additional instrumentation would need to be highly reliable and very stable in terms of drift.
- *Virtual Instrumentation:* One other possibility is the development of virtual instruments from information developed in the first principle system models. Certain parameters can be calculated based on physical instrumentation along with the resulting computations of the models. These virtual instruments could be presented to the operators to assist with decision making or as a replacement for failed or degraded physical instruments. These parameters would also be used in the diagnostic methodologies of the COSS.

### 5.3 Real-time Sensor Validation and Fault Diagnosis

In the present COSS prototype the implementation of functions for identifying failing sensors and for diagnosing equipment faults is limited to the demonstration of proof-of-principle capability. However, a number of issues will need to be addressed in future work to achieve robust and reliable COSS capabilities. While in principle there are no limits on the ability of the present algorithms to detect failing sensors and to identify faulty components given a sufficient sensor set, there are several aspects of power plant operation that will affect the realized sensitivity and localization capabilities of the algorithms.



These are identified below and need to be addressed in future work to advance the development to the next level of technology readiness.

- *Sensor Validation Algorithms:* A number of real-world considerations will be addressed in future development of the sensor validation algorithms. These are described below.

*The algorithms provide the potential for the COSS, as compared to an operator, to lower the threshold for detecting a failing sensor given the normal signal variation and noise present in the plant. Simulations that include models for noise will be used to determine performance limits. Ultimately, however, only experience with actual plant sensor measurements can provide the realistic signal environment needed to ensure these aspects have been effectively addressed. Long-term plans should include tests with utility plant data to address this.*

A formal means will be developed for discriminating between a failing sensor and a faulted component. An appropriate method would recognize that the incidence of sensor and component failure is infrequent and that these are isolated events and with high probability multiple failure are unlikely to coincide in time. Under these conditions a single sensor failure would be recognized with high probability by the signal validation algorithms and quite likely by the component fault diagnosis algorithms. Also, an equipment fault will produce a very conclusive result from the component fault diagnosis algorithms measurement data stream. But it could conceivably also result in the signal validation algorithms registering many sensors failing simultaneously. This could be discredited based on the low expectation for multiple sensor faults and the single equipment fault diagnosis. These are the types of rationales that might be used to treat the challenging problem of distinguishing sensor failures from equipment faults.

In practice at any time there will be some subset of plant sensors that are in a degraded state. Thus the training phase, where the normal relationship among sensor values is acquired, will inadvertently use these corrupted values. Potentially this can create a difficulty and so this possibility needs to be addressed if a reliable capability is to be achieved. One approach is to identify a “time-zero”, the time for learning the relatedness among sensor. Then any further degradation subsequent to time-zero would be successfully detected and the associated change in sensor condition identified. It also must be recognized that periodic maintenance on the plant can alter relations among sensors (e.g., a plant system is reconfigured or plant equipment is serviced). At this time it may be necessary to re-learn the relationship among sensors, i.e. to define a new time-zero.

The reporting of algorithm findings to the operator represents a human factors challenge. Past experience indicates that false alarms from an operator aid system cause the operator to distrust information from the operator aid system thereby lessen its effectiveness. While the frequency of false alarms is algorithm dependent and no false alarms is not realizable, providing continual expectation for the likelihood of a false alarm could allow the operator to better judge the reliability of information. Such an indication could be based on information about current maintenance activities. Such activities will tend to increase the likelihood that the last time zero learned state has been invalidated by, for example, a reconfiguration of equipment causing the algorithms to be less reliable.

- *Equipment Fault-Diagnosis Algorithms:* As is the case for signal validation above, a number of “real-world” considerations enter into the development of equipment fault-diagnosis algorithms. The time-selection window used for detecting the onset of an equipment fault is presently deterministically based which is acceptable for operation using plant data generated through

simulation. Actual plant data, however, contains noise and so the time-window selector will need to be appropriately generalized to reflect this.

There needs to be a means for assigning and optimizing sensor layout. Methods are needed to identify this sensor set and ensure a stated minimum performance for diagnosing equipment faults is achieved. Such a method would take the PID as input.

Some facility for auto-testing should be provided. That is, synthetic errors representative of perturbations caused by a fault are injected downstream of the measurement and algorithm performance for diagnosing this fault is evaluated.

The time-selection window is presently closed upon control system action subsequent to detection of an equipment fault. This limitation needs to be removed.

- *Bridge to Algorithms:* The current COSS prototype does not yet have a real-time interface to the sensor validation and the equipment fault diagnostic algorithms. Rather, this capability has been simulated in the current version of the prototype due to the difficulty of interfacing these independent software systems. The next step in the prototype development is to implement a real-time interface to demonstrate that the sensor validation and fault diagnosis algorithms can indeed operate in a real-time environment at the pace of actual plant faults and transients.
- *Expanded Fault Injection:* The COSS prototype is currently limited in the scope of plant faults for which it can assist an operator. As the COSS concept is proven to be a useful addition to control rooms, it will be desirable to expand the types of sensor and equipment faults that can be injected and then detected. These additions will maximize the value of a COSS and make it applicable to the complete spectrum of faults for which the operator could benefit from assistance for conducting mitigation actions.

## 5.4 COSS Human Factors Evaluation

The prototype represents a software collection of the different elements of the COSS, integrated in a manner that attempts to keep the advantages of the individual elements. The assembly of these elements into the integrated COSS represents initial design decisions. However, it was found in this work that in many cases, the COSS was a first-of-a-kind prototype, and applicable design standards could not be readily referenced. A human factors evaluation can help address unknown aspects of the design to arrive at an effective COSS.

The development of each COSS element suggested divergent design paths. While only one design was ultimately executed for each element in the prototype, the alternative designs deserve further evaluation and serve as a research roadmap for optimizing the COSS. Some of the alternative design considerations are discussed below:

- *Digital Alarm System:* The design adopted in the prototype maintains the annunciator tile approach common in conventional control rooms. As with annunciator boards, the design assumes the tiles should always be visible. Due to the constraint of only having a single DCS display available for the COSS, this resulted in designating a small area of the display for the tiles. The resulting tiles are quite small, although the labels are designed to be legible with normal visual acuity from a distance of 6 feet. It is unknown the extent to which a larger alarm tile or a different alarm presentation (e.g., alarm lists or plant health “radar” meters) would affect operator



performance in using the system. The alarm presentation will be the subject of future human factors research on the COSS.

The alarm tiles also feature trend lines to allow the operator to understand at a glance why an alarm may have sounded. Along with the trend lines are vertical tick marks and values to denote low and high warning and alarm states. The live value of the sensor is also presented prominently as a number at the bottom of each tile. This design was selected to present important historic (trending) information and set points with minimal visual clutter. The value of tracking such information and the utility of the trend within an alarm has not been tested on actual operators. Alternate scaling, line guides, and set point presentations should be reviewed to ensure the design is usable by operators.

Currently, the prototype alarm system also features blue confidence intervals to display information from multiple sensors. The blue color is distinct and, when there is sensor drift or failure, the span between sensors is readily apparent. The prototype does not provide additional guidance beyond the display of the sensor range. The design team reviewed several opportunities for providing sensor selection or incorporating a sensor voting system. Some of these systems have the potential to increase the complexity of the HSI when eliminating particular sensors. The value of such added functionality to the operator needs further exploration.

- *Computer-Based Procedures:* The COSS CBP closely follows traditional paper procedures, primarily adding in-line sensor information and soft controls relevant to each step. There are a number of design questions regarding the best way to present in-line information, completed steps, continuous actions steps, and soft controls, as well as the navigation between procedures and the ability of the operator to execute steps out of sequence. Many of these issues are being addressed by a separate LWRs research project on CBPs [14].

Beyond stand-alone CBP systems, the COSS recommender system affords the opportunity to present procedural steps in a non-traditional manner. For example, the recommender system already highlights the components in question and the preferred method of mitigating problems in the P&ID view. It may be possible to combine the recommender system with the CBP system in a more seamless manner. The best manner of guiding the operator through the procedures and the strengths and weaknesses of a combined recommender system with CBP remain important potential research topics.

- *Piping and Instrumentation Diagram:* The P&ID as implemented in the COSS is a relatively standard DCS P&ID, although special care was taken to ensure a well laid out and usable HSI. Additionally, the COSS features some highlighted information from the recommender system when diagnosing faults. A number of design questions arose during the design of the COSS, including the optimal level of detail to provide in the P&ID. Should the P&ID be simplified to only those components that can be controlled or measured, or should additional detail be provided to give greater context to the operator? The prototype adopts a simplified approach, but it may be desirable for operators to be able to zoom in for greater detail.

The prototype P&ID also does not provide any navigation between P&IDs, since the CVCS could be represented in a single display. It is assumed that the convention of having a link to another P&ID would work well for a more complex process flow diagram. Moreover, the functionality of opening another P&ID view would be compatible with the design element of tabs used throughout the COSS, whereby different system P&IDs would be denoted by different tabs along the top of the main display window. This would facilitate ready navigation between P&IDs if

needed. Future versions of the COSS prototype will explore different means of navigation between for systems that require multiple P&IDs.

A third P&ID area for design exploration centers on the interaction of the recommender system with the P&ID. While the current design features highlighting of specific components, there may be greater opportunity to embed the recommender system directly into the P&ID display. This must be done obviously yet unobtrusively to the operator. Future versions of the COSS prototype will explore the possibility of greater integration of the recommender system and the P&ID.

- *Recommender System:* The recommender system as currently deployed behaves as a type of ghost agent, whereby it monitors plant states in the background and attracts the operator's attention whenever something appears to be malfunctioning. The recommender system cannot take actions and relies on alerting the operator to the need to take action. This section has already mentioned potential enhancements to the recommender system through its interface with the CBP and P&ID systems. There remain significant opportunities to further enhance the recommender system through its mode of communication with the operator (e.g., addition of verbal alerts), through its diagnostic algorithms (e.g., offering a more sophisticated prognostic abilities), and its ability to respond with best case recommendations even for situations that fall outside the operating procedures (e.g., positing mitigation strategies for beyond design basis accidents). Additional capabilities of the recommender system as well as operator interactions with it will be explored in future research.

Solid human factors engineering practices without evaluation can only go so far in optimizing the design of a new system. Human factors evaluations will consist of two stages:

- *Formative evaluation early in the design process:* Such evaluations, which have been conducted informally during the initial mockups, use human factors engineers and process experts to conduct a heuristic evaluation of the system. A heuristic is simply a shorthand for an important design characteristic. Formal heuristic evaluations include a checklist of human factors considerations, against which the subject matter experts evaluate the HSI. For example, a common heuristic is consistency of the interface. Human factors experts and process experts can review the interface and then determine the extent to which the HSI elements follow a common, consistent look and feel. These evaluations are done early and frequently in the design process to ensure the overall quality of the design.
- *Summative evaluation of the prototypes:* Such evaluation, using qualified operators, actually tests the functionality and interactivity of the HSI. The purpose of the summative evaluation is to verify the prototype works as designed and that the design serves the needs of the operators. During such an evaluation, operators will typically run through a series of scenarios to test their interaction with the system. Performance metrics such as response time and errors are recorded during the scenario walkthroughs. Subjective measures such as operator preference may also be gathered. Finally, during a debrief, open-ended questions about the interface are asked in order to gather feedback and recommendations from the operators. Rarely will the first summative evaluation fail to reveal suggestions for improvement. As part of an iterative design cycle, the findings from the summative evaluation are translated into design recommendations. These design recommendations serve as the starting point for future versions of the system.

A formal formative evaluation of the COSS prototype is planned after the completion of this report. Subsequent to design improvements to the prototype from the formative evaluation, a summative evaluation with plant operators is planned.



## 6. References

1. Quinn, T., Bockhorst, R., Peterson, C., Swindlehurst, G. (2012). "Design to Achieve Fault Tolerance and Resilience," INL/EXT-12-27205. Idaho Falls: Idaho National Laboratory.
2. Büttner, W. E., Advanced Computerized Operator Support Systems in the FRG, IAEA Bulletin, Autumn, 1985.
3. Berg, Oivind, Operator Assistant – A Conceptual Outline, OECD Halden Reactor Project, HWhP-032, 2012.
4. Eascon Corporation web page, <http://www.eascon.it>, Bologna, Italy, 2013.
5. U.S. Department of Transportation, Federal Aviation Administration, Introduction to TCAS II Version 7.1, 2011.
6. U.S. Department of Transportation, Federal Aviation Administration, Advanced Avionics Handbook, FAA-H-8083-6, 2009.
7. Institute of Nuclear Power Operations (INPO), SOER 10-2 Engaged, Thinking Organization, Atlanta, GA, 2010.
8. Electric Power Research Institute (EPRI), "Disturbance Analysis and Surveillance System (DASS) Scoping and Feasibility Study," EPRI NP-2240, Palo Alto, California, July 1982.
9. International Atomic Energy Agency, "Development and Implementation of Computerized Operator Support Systems in Nuclear Installations," Vienna, Austria, September 1994.
10. R. B. Vilim, A. M. Heifetz, D. Yun, and L. Yacout, "Description of Algorithms for Detecting Sensor Degradation and Preliminary Tests Using Simulations," ANL/NE-13-2, February 1, 2013.
11. R. B. Vilim, A. M. Heifetz, Y. S. Park, and J. Choi, "Description of Fault Detection and Identification Algorithms for Sensor and Equipment Failures and Preliminary Tests Using Simulations," ANL/NE-12/57, November 30, 2012.
12. Institute of Electrical and Electronics Engineers (IEEE), IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities, IEEE 1786, New York, New York, 2011.
13. Ulrich, T., Boring, R., Phoenix, W., DeHority, E., Whiting, T., Morrell, J., and Backstrom, R. (2012). "Applying Human Factors Evaluation and Design Guidance to a Nuclear Power Plant Digital Control System," INL/EXT-12-26797. Idaho Falls: Idaho National Laboratory.
14. Oxstrand, J. and Le Blanc, K. (2012). Computer-Based Procedures for Field Workers in Nuclear Power Plants: Development of a Model of Procedure Usage and Identification of Requirements. Idaho National Laboratory External Report. INL/EXT-12-25671, Rev. 0.

## **Appendix A: Computerized Operator Support System Specifications**

### **A.1 General COSS Interface Specifications**

#### **Purpose**

The COSS interface displays all the screen elements necessary to warn the operator about faults, provide the operator with a diagnosis of faults, provide mitigation actions to address faults, and interaction methods to complete computer-based procedures and manually adjust components.

#### **Design Assumptions**

1. The COSS shall be located on the simulated control board within the control panels associated with the CVCS.
2. The dimensions of the COSS shall be 1280 pixels in width and 720 pixels in height.
3. The COSS shall contain digital indicators and soft controls.

#### **Design Requirements**

1. The main window of the COSS display featuring the computer-based procedures, P&IDs, and trend alarms shall have the dimensions of 1100 pixels in width and 600 pixels in height.
2. The main window shall display computer-based procedures, P&IDs, and trend alarms.
3. The top section of the COSS display featuring the COSS status display, navigation buttons, and recommender system shall have the dimensions of 100 pixels in width and 100 pixels in height.
4. The right section of the COSS display featuring the trend alarms shall have the dimensions of 180 pixels in width and 720 pixels in height.
5. Lucida Sans UI font shall be used for all text displayed on the COSS.
6. Yellow-Green shall be reserved for the recommender system to display fault warnings and highlight fault-affected components on the P&IDs displayed in the main window.
7. Black, white, and shades of grey and pale color tones shall be used throughout the COSS to maintain a dull screen.
8. Light blue lines shall be used to indicate piping between components.
9. Black lines shall be used to indicate electrical buses.
10. Muted Yellow will be used to indicate Lock Out Tag Out information.
11. Blue shall be reserved to represent sensor drift and failure.
12. Yellow shall be used to represent that a component's indication value has reached a warning set point.
13. Red shall be used to represent that a component's indication value has reached an alarm set point.

### **A.2 Computer-based Procedures Specifications**

#### **Purpose**

The computer based procedure allows the operator to follow plant procedures using an electronic place keeping system. The computer based procedure features inline plant status information and soft controls to allow the operator to make decisions and perform actions within the procedure display area.

## Design Assumptions

1. The computer-based procedure shall occupy the main window area of the COSS display.
2. The computer-based procedure shall follow the style conventions for COSS.
3. The computer based procedure window shall be accessible at all times from the COSS menu and from the COSS recommender system when appropriate.
4. The computer-based procedures shall follow the style and formatting conventions of the existing paper procedures.
5. The computer based procedure shall allow multiple simultaneously open procedures.

## Design Requirements

1. The computer based procedure window shall be active when the “Procedure” button is selected in the COSS menu.
2. When the operator clicks the “Procedure” button, the main window shall display the last active procedure.
3. When the operator is guided to a procedure by the COSS recommender system, the applicable procedure shall open in the main window. The “Procedure” button on the COSS menu shall be selected when the procedure is activated.
4. Each procedure shall feature a tab at the top of the display, which shall be visible at all times that the procedure window is active. This tab shall feature the procedure number (e.g., AOP-016). A white background shall be used to for the active procedure tab.
5. Multiple procedures shall be accommodated by additional tabs featuring grey backgrounds.
6. If no procedure is currently open, the window shall display centered in large type “No Procedure Currently Open”. The bottom right of the window shall feature a button labeled “Procedure List”. When pushed, this button shall provide a menu of available plant procedures. (The button will be displayed, but the function will not be enabled for the initial prototype.)
7. When displaying a procedure, the procedure name shall be identified at the beginning of each procedure with a boldfaced, centered heading (e.g., AOP-016, Excessive Primary Plant Leakage).
8. Following the heading, the procedure shall display the Purpose and Entry Conditions. Each shall feature a boldfaced heading followed by a checkbox or checkboxes for what condition was met.
9. The procedure steps shall be listed under the heading “Operator Actions”.
10. The procedure shall feature a button at the bottom right labeled “Close Procedure”. When pushed, this button shall pop-up a confirmation dialog box that the operator wants to close the procedure. The procedure shall feature a second button to the immediate left entitled “Procedure List”. These buttons shall always be visible when the procedure is displayed.
11. The procedure shall feature a two-column format, with a boldfaced, underlined heading to indicate the Action and Response Not Obtained columns.
12. The procedure steps shall be numbered in Arabic numerals. Only the Action column shall be numbered. Substeps shall be lettered in alphabetical sequential order.
13. Each procedure step shall include a check box next to the instructions for the Action and Response Not Obtained columns. Each substep shall also feature a checkbox. The checkbox is automatically checked when the operator selects the go to next step button.
14. As many steps should be visible as possible. This means that the system will display steps before and after the current step as possible.
15. The display area shall be scrollable up or down (as appropriate) to accommodate steps before and after the current step. The display area should support drag scrolling for touch-based interfaces. The buttons at the bottom right of the window (i.e., “Procedure List” and “Close Procedure”) shall continue to be visible when scrolling and will reside outside the scrollable area.
16. The current step shall be highlighted with a light grey background.

17. Appropriate plant status shall be displayed below each current step (e.g., RHR is not in operation). The plant status indication shall be clearly differentiable from buttons.
18. Plant status indicators shall be updated only for the currently selected step. Once a step is completed, the plant status shall retain the value at the time the procedure step was completed. Procedure steps that have not been accessed shall display a plant status indication of "TBD". Currently active status indicators shall feature active (e.g., black) text. Inactive status indicators shall feature inactive (e.g., grey) text.
19. Below each current step shall be provided a button that advises the next step to be taken (e.g., Go to Step 3.)
20. Upon pressing the next step button, the appropriate checkboxes shall be checked within the current step. The selectable button(s) in the current step shall be disabled. The highlight shall advance to the next appropriate step, update applicable plant status information, and enable the appropriate buttons for that step.
21. Links to other procedures shall call up a new procedure tab for that procedure.
22. Continuous action steps shall be indicated with a star in front of the left column checkbox. These steps shall provide a button as follows: "Monitor Step with COSS". A list of continuous action steps shall be maintained on a separate COSS tab in the procedure window.
23. Procedure steps that require actions to be performed in a specified time window shall display the available time as system status. The step shall feature a button entitled: "Activate Shot Clock with COSS". Clicking on this box shall activate a Shot Clock in the COSS area.
24. Actions currently being performed shall be denoted with an in progress indication.
25. Unavailable buttons shall be disabled, e.g., a non-applicable button in the Response Not Obtained column will be visible but not enabled.
26. The operator may click on a procedure step out of sequence. The system shall then prompt the operator with a dialog box to ensure that the operator wishes to abandon the procedure sequence. Upon operator confirmation, subsequent, previously performed procedure steps shall then be unchecked.
27. The operator may enact automatic execution of a sequence of steps. Buttons that run the automatic execution and stop the automatic execution shall be included in an area along the bottom of the CBP.
28. The CBP shall display a text message near the run and stop buttons describing the sequence of the steps that can be automatically executed.

## **A.3 P&ID Display Specifications**

### **Purpose**

The P&ID provides a graphical depiction of the functional relationships between CVCS components. The COSS recommender system uses the P&ID to highlight components affected by the fault. Additionally, the P&ID provides an interaction method to manually adjust components through pop-up menus.

### **Design Assumptions**

1. The P&ID display shall occupy a portion of the main window area of the COSS display.
2. The P&ID display shall follow the style conventions for the COSS.
3. The P&ID display shall use standard engineering symbols to represent components.



## Design Requirements

1. The components shall be physically arranged on the display based on functional relationships between components.
2. A dull grey consistent with COSS style conventions shall be used for the background.
3. Light blue lines shall be used to represent pipes connecting components.
4. Muted yellow shall be used to represent lock-out tag-out information.
5. Only functionally important and main control room relevant connections between components shall be included in the P&ID display.
6. Components shall be displayed with a shade of grey darker than the background grey. Components shall be outlined with white lines.
7. Static black component labels shall be positioned near or within the associated component.
8. Dynamic values shall be presented in black text and preferably with a white background where space allows. The value units shall be displayed to the right of the value in black text or right-aligned underneath the value.
9. White shall be used to represent valves in the open position.
10. Black shall be used to represent electrical equipment in the energized state.
11. Each P&ID shall feature a tab at the top of the display, which shall be visible at all times the P&ID window is active. This tab shall feature the name of the P&ID displayed.
12. Multiple P&IDs shall be accommodated by additional tabs.
13. Buttons linking the displayed P&ID to functionally related P&IDs shall be displayed within the main window. The link buttons shall feature pipe connections to specific components within the displayed P&ID. A shade of grey lighter than the main window background shall be used for the linking button background.
14. Clicking the P&ID linking buttons shall display the associated P&ID in the main display window.
15. Pop-up menus shall be displayed when a component is clicked. These menus shall display detailed component information and buttons to make manual adjustments to the component.

## A.4 Recommender System Specifications

### Purpose

The primary purpose of the recommender system is to provide warnings, descriptions, and mitigation techniques for faults detected and diagnosed by the COSS. The recommender system serves as an online visual representation of the detection, validation, monitoring, and diagnosis COSS activities.

### Design Assumptions

1. The recommender system shall occupy a portion of the top window area of the COSS display.
2. The recommender system shall follow the style conventions for the COSS.
3. The recommender system shall always be visible on the COSS display.

### Design Requirements

1. The recommender system shall always be active.
2. The recommender system shall be divided into the warning and message sections bordered with a black line.
3. The recommender system shall display a blank grey background when no fault is detected.



4. When a fault is detected, the recommender system shall display the text “Warning” or “Alarm” and change the background of the warning area to green. A text message describing the fault shall be displayed within the warning section.
5. When a trending fault is detected a shot clock shall be displayed within the warning section.
6. The shot clock shall indicate the event that is anticipated to occur when the displayed time comes to 0. The shot clock text should be in black text with a white background.
7. If multiple faults are detected, the fault text description with the greatest safety implications will be displayed.
8. The warning section shall contain a text display of the number of faults and the priority level of the current fault displayed.
9. The warning area shall contain arrows to navigate between multiple faults.
10. In the duration between when the fault is detected and the COSS completes the validation and diagnosis functions a moving status bar shall be displayed.
11. If a diagnosis is successful, a description of the fault shall be displayed in the message section with an associated “Show Me” button. Clicking the button shall highlight fault related components on the main P&ID.
12. A toggle button labeled “CVCS Overlay” shall be displayed on the main P&ID to toggle between COSS diagnosed component highlighting and standard P&ID views.
13. The second highest priority fault shall be displayed after the COSS determines the highest priority fault has been successfully mitigated.
14. If a diagnosis is unsuccessful and no root cause is identified, “Diagnosis Failure”, shall be displayed in the message section.
15. The suggested mitigation actions shall be displayed below the diagnosis.
16. The mitigation action that ensures the greatest plant safety shall be displayed above alternative and more conservative mitigation actions.
17. Each mitigation action shall have an associated button containing the text “Show Me” along with the name of the procedure required for the mitigation action. Clicking the button displays the corresponding procedure in the main window area.
18. A “Disregard” button shall be displayed within the message section to provide warning acknowledgment and manual mitigation actions.
19. A reset button shall be displayed to reset the warning.
20. The recommender system shall display “Steady State Operations Resumed” after the COSS has determined all detected faults were successfully mitigated.

## **A.5 Trend Alarms Specifications**

### **Purpose**

The trend alarms provide warning and alarms to the operator when a component reaches the appropriate set point. The trend alarms also provide the operator with online trend information for their associated components.

### **Design Assumptions**

1. The trend alarms shall occupy the right portion of the COSS display.
2. The trend alarms shall follow the style conventions for the COSS.
3. The trend alarms shall be visible at all times.

## **Design Requirements**

1. The trend alarm for each component shall feature the components label in black text, right justified, along the top of the trend alarm.
2. Each trend alarm shall display the current indication value along the bottom of the trend alarm in black text.
3. Each trend alarm shall display historical indication values in the form of a trend line.
4. Each trend alarm shall use grey to denote the current indication value is within normal operating ranges, yellow to denote the current indication has reached the warning set point, and red to denote the current indication has reached the alarm set point.
5. Component set points shall be depicted as ticks on the right side of the trend alarm.
6. The absolute range for each component shall be displayed as a bracket with numerical text displays of the absolute range values. The bracket and absolute range values are situated along the left side of the trend alarms.
7. Each trend alarm shall use blue confidence intervals around the multiple indicator sensor values associated with each component to show sensor drift and faults.
8. Clicking a trend alarm shall display an enlarged and more detailed version in the main window area. These enlarged and more detailed versions include set point values near the set point tick marks. Multiple trend alarms shall be presented on the same plot on the main window. Selected trend alarms displayed in the main window shall have the smaller trend alarm along the right section of the screen highlighted with a white border.

## **A.6 Navigation Specifications**

### **Purpose**

The navigation system provides the operator with the ability to change views between the computer based procedures, P&IDs, and detailed trend alarms.

### **Design Assumptions**

1. The navigation system shall occupy the main menu area of the COSS display at the top of the window.
2. The navigation system shall follow the style conventions for the COSS.

### **Design Requirements**

1. The navigation system buttons shall always be visible and active.
2. When selected, the navigation buttons shall be outlined with a white border.
3. A procedure button shall display the last active procedure when selected. If no procedure is active, "No Active Procedure" is displayed in the main window area.
4. A P&ID button shall display the last active P&ID when selected.
5. A trend button shall display the last active trend alarm when selected. If no trend alarm is active, "No Active Trend Alarm" is displayed in the main window area.

## **A.7 COSS Status Display Specifications**

### **Purpose**

The COSS status display provides the operator with real time feedback indicating the status of the COSS. The status display freezes to serve as a visual indication that the COSS display encounter an error and is no longer functioning properly.

### **Design Assumptions**

1. The COSS status display shall occupy a small portion of the top left window area of the COSS display.
2. The COSS status display shall follow the style conventions for the COSS.
3. The COSS status display shall always be visible on the COSS display.

### **Design Requirements**

1. The COSS status display shall contain the text “CVCS COSS” in black text.
2. The “COSS” text shall be highlighted with a pulsing green color and a pulsing green circle shall be displayed near the “COSS” text.
3. The COSS highlighting and a circle next to the status display text shall pulse at a slow rate.
4. The pulsing shall alternate between the grey background and the green color
5. If the COSS becomes unresponsive, the pulsing shall cease and the current highlighted state of the “COSS” text and a static green circle shall remain on the display.